Emulex Driver and Utilities for Linux

Version 8.1.10.3

HBAnyware Version 3.2

User Manual

Copyright© 2007 Emulex Corporation. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Emulex Corporation.

Information furnished by Emulex Corporation is believed to be accurate and reliable. However, no responsibility is assumed by Emulex Corporation for its use; or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of Emulex Corporation.

Emulex, AutoPilot Installer, BlockGuard, cLAN, FabricStream, FibreSpy, Giganet, HBAnyware, InSpeed, IntraLink, LightPulse, MultiPulse, SAN Insite, SBOD and Vixel are registered trademarks, and AutoPilot Manager, EZPilot, SLI and VMPilot are trademarks of Emulex Corporation. All other brand or product names referenced herein are trademarks or registered trademarks of their respective companies or organizations.

Emulex provides this manual "as is" without any warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Emulex Corporation may make improvements and changes to the product described in this manual at any time and without any notice. Emulex Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties that may result. Periodic changes are made to information contained herein; although these changes will be incorporated into new editions of this manual, Emulex Corporation disclaims any undertaking to give notice of such changes.

Installation 1

Driver Information 1
- Supported Features 1
- New Features in this Release 1
- Prerequisites 2
  - For the lpfc Driver Kit 2
- Compatibility 2
- Things to Know Before You Download 2
- Known Issues 2

Installing the Driver Kit 3
- Driver Kit Install Script Options 4
- Driver Kit Directory Structure 4

Installing the Driver on Unsupported Linux Distributions 4

Upgrading the Kernel or Applying a Distribution Service Pack or Update 5
- Installing the Driver Kit into an Upgraded Kernel 5

Booting From a Non-Zero LUN Attached to an Emulex HBA 6

Installing the Applications Kit 7
  - Prerequisites 7
  - Procedure 7
  - Utilities Directory Structure 7
- Installing the HBAnyware Utility with Web Launch 8
  - Prerequisites 8
  - Procedure 8
- Installing the HBAnyware Security Configurator 9
  - Prerequisites 9
  - Procedure 9
- Uninstalling the Driver Kit 10

Uninstalling the Applications Kit 11
- Uninstalling the HBAnyware Security Configurator 11
- Uninstalling HBAnyware with Web Launch 11
- Uninstalling HBAnyware and lputil 11

Configuration 12

Introduction 12
- Starting the HBAnyware Utility for Linux 13
  - Starting the HBAnyware Utility 13
  - Starting the HBAnyware utility with Web Launch 13
  - Starting the HBAnyware Security Configurator 14
  - Starting the HBAnyware Utility from the Command Line 14
- Changing Management Mode 15
- The HBAnyware Utility Window Element Definitions 16
  - The Menu Bar 16
  - The Toolbar 16
  - The Toolbar Buttons 16
  - The Discovery-Tree 17
  - Property Tabs 18
  - Status Bar 18
- Using the the HBAnyware Utility Command-Line Interface 18
  - Using the CLI Client 18

The CLI Client Command Reference 20
Starting the lputil Utility 33
Discovering HBAs 34
Discovering HBAs Using the HBAnyware Utility 34
Configuring Discovery Settings 35
Discovering HBAs Using the lputil Utility 36
Sorting HBA Information 36
Sorting HBAs Using the HBAnyware Utility 36
Sort by Host Name 36
Sort by Fabric Address 37
Sorting Local HBAs Only Using the HBAnyware Utility 37
Sorting Local HBAs Using the lputil Utility 37
Viewing HBA Information Using the HBAnyware Utility 37
Viewing Discovery Information 37
Discovery Information Field Definitions 38
Viewing Host Information 38
The Host Information Tab 39
The Host Driver Parameters Tab 39
Viewing General HBA Attributes 40
Adapter Summary Field Definitions 41
Adapter Status Area Field Definitions 41
Viewing Detailed HBA Information 42
Adapter Details Field Definitions 42
Port Attributes Field Definitions 43
Loop Map Table Definitions 43
Viewing Fabric Information 43
Discovery Information Field Definitions 44
Viewing Target Information 44
Viewing LUN Information 45
LUN Information Field Definitions 46
Viewing Port Statistics 46
Port Statistics Field Definitions 47
Viewing Firmware Information 48
Firmware Field Definitions 49
Viewing Target Mapping 50
Target Mapping Field Definitions 50
Viewing HBA Information Using the lputil Utility 51
Resetting HBAs 52
Resetting the HBA Using the HBAnyware Utility 52
Resetting the HBA Using the lputil Utility 52
Updating Firmware 53
Updating Firmware Using the HBAnyware Utility 53
Prerequisites 53
Procedure 53
Updating Firmware (Batch Mode) Using the HBAnyware Utility 55
Prerequisites 55
Procedure 55
Updating Firmware Using the lputil Utility 56
Prerequisites 56
Procedure 57
Enabling or Disabling an HBA's BIOS 57

Enabling or Disabling an HBA's BIOS Using the HBAnyware Utility 57
Enabling or Disabling an HBA's BIOS Using the lputil Utility 59
Configuring the Driver 60
Setting Driver Parameters Using the HBAnyware Utility 60
Setting Driver Parameters for an HBA 60
Setting Driver Parameters for a Host 62
Creating the Batch Mode Driver Parameters File 63
Assigning Batch Mode Parameters to HBAs 64
Driver Configuration Methods Using modprobe and /etc/modprobe.conf 66
Temporary Configuration Method 66
Persistent Configuration Method 66
Temporary Driver Configuration by Read/Write to sysfs 66
Creating a New Ramdisk Image 67
For Installed lpfc Driver Kits 67
For Distribution In-Box lpfc Drivers 68
Dynamically Adding LUNs and Targets 68
Downloading PCI Configuration 68
Driver Parameters Reference Table 69
Viewing Target Mapping 71
Using udev for Persistent Naming 72
Using udev to Discover Logical to Physical Mappings for sd Devices 72
Configuring the System to Boot From SAN Using Persistent Names 72
Using udev with st Devices 72
Further Information About Persistent Names 74
Performing Diagnostic Tests Using the HBAnyware Utility 75
Running a Quick Test 76
Running a POST Test 76
Using Beaconing 76
Creating Diagnostic Dumps 77
Displaying PCI Registers and Wakeup Information 78
Running Advanced Diagnostic Tests 78
Running Loopback Tests 79
Running End-to-End (ECHO) Tests 81
Saving the Log File 82
Out-of-Band SAN Management 83
Adding a Single Host 83
Adding a Range of Hosts 84
Removing Hosts 85
HBAnyware Security 86
Introduction 86
Starting the HBAnyware Security Configurator 86
Prerequisites 86
Procedure 87
Running the Configurator for the First Time/Creating the ACG 87
Designating a Master Security Client 88
Access Control Groups 88
Introduction 88
Access Control Group Tab on the MSC 88
Access Control Group Tab on a Non-MSC 89
ACG Icons 89
Run the Configurator for the First Time/Create the ACG 90

Adding a Server to the ACG 90
Deleting a Server from the ACG 91
Removing Security from all Servers in the ACG 91
Generating New Security Keys 91
Restoring the ACG to Its Last Saved Configuration 92
Accessing a Switch 92
Access Sub-Groups 92
Introduction 92
ASG Icons 93
Creating an ASG 93
Reserved Indices - Examples 94
Adding a Server to an ASG 94
Deleting an ASG 95
Restoring an ASG to Its Last Saved Configuration 95
Editing an ASG 95
About Offline ASGs 97
Backup Masters 97
Introduction 97
Backup Master Eligible Systems 98
Backup Master Tab and Controls 98
Creating a Backup Master 98
Reassigning a Backup Master as the New MSC from the Old MSC 99
Reassigning a Backup Master as the New MSC from the Backup Master 100

Troubleshooting 101

Introduction 101
Unusual Situations and their Resolutions 101
General Situations 101
Security Configurator Situations - Access Control Groups (ACGs) 106
Security Configuration Situations - Access Sub-Groups (ASG) 107
HBAnyware Security Configurator Situations - Backup Masters 109
Error Message Situations 110
Master Security Client Situations 111
lpfc Log Messages 112
Introducton 112
Message Log Example 113
ELS Events (0100 - 0199) 113
Link Discovery Events (0200 - 0299) 117
Mailbox Events (0300 - 0399) 124
Initialization Events (0400 - 0499) 130
FARP Events (0600 - 0699) 134
FCP Traffic History (0700 - 0799) 134
Node Table Events (0900 - 0999) 138
Miscellaneous Events (1200 - 1299) 139
Link Events (1300 - 1399) 140
IOCTL Events (1600 - 1699) 141

Installation

Driver Information

Supported Features

- SNIA-CTP compliant SMI-S 1.1 Provider
- Topology support: FC-AL, point-to-point, fabric with auto-topology negotiation
- Support for 1, 2 and 4 gigabit (Gb) with auto-rate negotiation
- Protocols: SCSI-FCP, FCP-2 (FC-Tape profile, including use of ADISC instead of PLOGI), FC initiator mode
- Tested up to thirty-two host bus adapter (HBA) ports
- Monitoring and parameter configuration using Emulex's HBAnyware™ graphical user interface utility or parameter configuration using Emulex's hbacmd command-line interface utility
- Parameter configuration using Emulex's LightPulse® diagnostic utility (lputil) command-line interface utility
- Support for Common HBA API
- Batch firmware download capability
- Support for the sysfs interface
- PCI hot plug support
- Vital Product Data (VPD) support
- “Linux Tools” link on the Linux portion of the Emulex Web site (visit the link to see the available tools)

New Features in this Release

The Emulex version 8.1.10 driver for Linux includes the following enhancements:

- Red Hat Enterprise Linux 5 support
- HBAnyware utility version 3.2 which enables the local and “in-band” discovery of Emulex and OEM branded Emulex HBAs. The HBAnyware utility also supports Virtual Connect technology which delivers virtualized server I/O connections to Fibre Channel (FC) based SAN networks as well as to Ethernet networks for Linux systems. See page 12 for more information about the HBAnyware utility.
- Easier driver installation requiring fewer installation steps
- Packaging is different from previous versions of the 8.1 driver. The Application Helper Module is no longer needed and was removed.
- The utilities installation includes an upgrade kernel option
- Improved target queue full driver throttling
- Improved SCSI I/O abort wait strategy
- Implements blocking SCSI I/O during error recovery
- Improved HBA outstanding command handling
- Implements HBA GetFcpTargetMapping function for the HBA API

Prerequisites

For the lpfc Driver Kit

To install the lpfc driver kit, the appropriate distribution kernel development packages must be installed for the currently running kernel, which include the gcc compiler and the kernel sources.

The lpfc driver kit supports the following distributions:

- Red Hat Enterprise Linux 5 (Intel x86, Intel Itanium2, Intel EM64T, AMD64, and PowerPC 64-bit architectures).
- SuSE Linux Enterprise Server 10 SP1 (Intel x86, Intel Itanium2, Intel EM64T, AMD64, and PowerPC 64-bit architectures).

Compatibility

- LPe11000, LPe11002 and LPe1150 (minimum firmware version 2.50a4. Firmware version 2.70a5 is recommended for best performance.)
- LP11000, LP11002 and LP1150 (minimum firmware version 2.10a10. Firmware version 2.70a5 is recommended for best performance.)
- LP1005DC-CM2 (minimum firmware version 1.90a5)
- LP10000ExDC and LP1050Ex (minimum firmware version 1.91a1)
- LP10000DC and LP10000 (minimum firmware version 1.91a1)
- LP1050DC and LP1050 (minimum firmware version 1.91a1)
- LP9802DC (minimum firmware version 1.91a1)
- LP9802 (minimum firmware version 1.91a1)
- LP982 (minimum firmware version 1.91a1)
- LP9402DC, LP9002DC, LP9002L and LP9000 (minimum firmware version 3.93a0)
- LP952L (minimum firmware version 3.93a0)

Things to Know Before You Download

- You must uninstall any previous lpfc driver kits and/or Application Helper Modules that were installed from the Emulex CD or downloaded from the Emulex Web site, (i.e. not part of a distribution), before installing this driver kit.

Known Issues

- Some Web browsers attempt to continually reload the HBAnyware utility’s online help rendering it unusable. In this case, disable the Web browser's JavaScript capability. Refer to the Web browser's documentation for instructions.
- Starting with HBAnyware version 3.2, Emulex provides support for LightPulse adapters that are reprogrammed with WWPNs outside the typical Emulex range, such as HP’s upcoming Virtual Connect for Fibre Channel on the BladeSystem c-Class platform. In such environments, HBAnyware version 3.2 must be deployed across all servers on the SAN, as well as any other management console used for out-of-band management, so that all adapters appear in the discovery tree.

Installing the Driver Kit

The lpfc-install script installs the lpfcdriver_2.6 RPM.

The RPM:

- Installs the driver source files to the /usr/src/lpfc directory.
- Builds the driver for the currently running kernel.
- Installs the driver to the proper directory for the currently running kernel.

Once the RPM is installed, the lpfc-install script creates a new ramdisk for the currently running kernel so that the lpfc driver is loaded when the kernel is initialized during system startup.

Note: You must uninstall any previous lpfc driver kits and/or Application Helper Modules that were installed from the Emulex CD or downloaded from the Emulex Web site, (i.e. not part of a distribution), before installing this driver kit. This installation will fail if a previous version of the lpfc driver or the Application Helper Module is detected.

Refer to “Uninstalling the Driver Kit” on page 10 and “Uninstalling the Applications Kit” on page 11 for more information.

When invoked without options, the 'lpfc-install' script automatically archives any driver that is shipped as part of the distribution's kernel during the installation procedure. Old drivers that are archived during installation are then restored when the driver kit is uninstalled.

Note: The HBAnyware and LightPulse (lputil) utilities are bundled together and must be installed separately from the driver. Refer to the "Installing the Utilities" on page 11 for more information.

Note: The lpfc-install script does not support custom kernels. For example, kernels with Version_Release strings that do not match those of the original distribution kernel.

To install the Emulex driver for Linux:

1. Install a supported Emulex HBA in the system. Refer to the HBA's Installation manual for specific hardware installation instructions.
2. Remove any previously installed lpfc driver kits and/or Application Helper Modules that were installed from the Emulex CD or downloaded from the Emulex Web site, (i.e. not part of a distribution’s kernel) before proceeding. Refer to “Uninstalling the Driver Kit” on page 10 and “Uninstalling the Applications Kit” on page 11 for more information.
3. Download the driver kit from the Emulex Web site or copy it to the system from the installation CD.
4. Log on as 'root' to a terminal, and unpack the tarball with the following command:

   ```
   tar xzf lpfc_2.6_driver_kit-<driver version>.tar.gz
   ```
5. Change to the directory that is extracted:

   ```
   cd lpfc_2.6_driver_kit-<driver version>/
   ```
6. Execute the 'lpfc-install' script with no options to install the new driver kit. Type:

   ```
   ./lpfc-install
   ```

Once the 'lpfc-install' script has completed successfully, the Emulex lpfc driver is loaded and Fibre Channel disks that are properly connected to the system are accessible. Reboot the system now to enable the newly added driver options in the ramdisk. You can also reboot the system later if you wish.

Driver Kit Install Script Options

The following options are available for use with the Emulex install script for Linux:

- -h,--help - Prints a help message describing command line parameters.
- -u,--uninstall - Uninstalls the currently installed driver kit.

Driver Kit Directory Structure

After installation, the following directory is created on the system.

Table 1: Driver Kit Directory Structure

Directory	Description
/usr/src/lpfc	Driver source files.

Installing the Driver on Unsupported Linux Distributions

The driver kit supports the Linux distributions listed on page 2. As of Linux kernel 2.6.12, the lpfc driver is distributed with the Linux kernel sources. To install the Emulex lpfc driver on an unsupported distribution of Linux, refer to the distribution's Web site or http://kernel.org.

Note: The Emulex version 8.1 driver for Linux is not intended for, and will not operate on, any kernel prior to 2.6.12. If you are using an earlier 2.6 kernel, you must use the Emulex driver for Linux version 8.0.16.x.

Upgrading the Kernel or Applying a Distribution Service Pack or Update

You can install the driver kit into an upgraded kernel. The installation of an update or service pack generally involves updating the kernel.

Note: Some distribution service packs or updates contain an Emulex driver. If the driver version contained in the distribution or service pack is the same version or newer than the currently installed driver kit, re-installation of the driver kit may not be necessary.

Note: The lpfc-install script does not support custom kernels. For example, kernels with Version_Release strings that do not match those of the original distribution kernel.

Note: Follow these steps before installing a new update CD to a distribution or applying a service pack to a distribution.

Installing the Driver Kit into an Upgraded Kernel

To install the driver kit into an upgraded kernel:

1. Execute the lpfc-install script with the '--uninstall' option. Type:

   ```
   /usr/src/lpfc-install --uninstall
   ```
2. Upgrade the kernel and/or distribution.
3. Reboot the system with the new kernel.
4. Download the driver kit from the Emulex Web site or copy it to the system from the installation CD.
5. Log on as 'root' to a terminal, and unpack the tarball with the following command:

   ```
   tar xzf lpfc_2.6_driver_kit-<driver version>.tar.gz
   ```
6. Change to the directory that is extracted:

   ```
   cd lpfc_2.6_driver_kit-<driver version>/
   ```
7. Execute the 'lpfc-install' script with no options to install the new driver kit. Type:

   ```
   ./lpfc-install
   ```
8. Reboot the system to complete re-installation of the Emulex driver.

Booting From a Non-Zero LUN Attached to an Emulex HBA

This section describes how to configure SLES 10 to boot from an FC attached disk device other than /dev/sda. This example uses /dev/sdb.

To boot from a non-zero LUN attached to an lpfc HBA:

1. Configure the Emulex HBA bootBIOS to boot from the desired LUN.
2. Start the standard SLES 10 installation.
3. At the Installation Settings screen, after configuring the desired partitions, select the **Expert** tab.
4. Select **Booting** to change the bootloader configuration.
5. The Boot Loader Settings window appears. Select the **Boot Loader Installation** tab.
6. In the section labeled Boot Loader Location, select **Other**, then select /dev/sdb from the drop-down box.
7. Click **Boot Loader Installation Details**. The Boot Loader Installation Details window appears. Select /dev/sdb and click **Up** to move /dev/sdb to the top of the list.
8. Click **OK**.
9. In the Boot Loader Settings window, Click **Finish**.
10. Proceed with the installation.

Installing the Applications Kit

Follow these instructions to install the Application Kit on your system. The Applications Kit contains the HBAnyware and lputil utilities.

Prerequisites

- The lpfc driver must be installed.

Procedure

To install the Applications Kit:

1. Log on as ‘root’.
2. Download the utilities from the Emulex Web site or copy them to the system from the installation CD.
3. Copy the ElxLinuxApps-<AppsRev><DriverRev>.tar file to a directory on the install machine.
4. Change (use cd command) to the directory to which you copied the tar file.
5. Untar the file. Type:

   ```
   tar xvf ElxLinuxApps-<AppsRev><DriverRev>.tar
   ```
6. Uninstall any previously installed versions. Type:

   ```
   ./uninstall
   ```
7. Run the install script. Type:

   ```
   ./install
   ```
8. Enter the type of management you want to use:

   ```
   1   Local Mode  : HBA's on this Platform can be managed by
       HBAnyware clients on this Platform Only.
   2   Managed Mode: HBA's on this Platform can be managed by local
       or remote HBAnyware clients.
   3   Remote Mode : Same as '2' plus HBAnyware clients on this
       Platform can manage local and remote HBA's.
   ```
9. You are prompted as to whether or not to allow users to change management mode after installation. Enter the letter 'y' for yes, or 'n' for no.

Utilities Directory Structure

After installation, the following directories are created on the system.

Table 2: Utilities Directory Structure

Directory	Description
/usr/sbin/lpfc	lputil utility files.
/usr/sbin/hbanyware	HBAnyware files.

Installing the HBAnyware Utility with Web Launch

Prerequisites

Before installing the HBAnyware utility with Web Launch, ensure your systems meet the following requirements. See page 12 for more information about the HBAnyware utility with Web Launch.

- The system on which you are installing the Web Launch services package (the server) requires the following:
  - The HTTP server must be configured to handle the JNLP MIME file type. The following MIME file type/file extension must be added to your server configuration:

    ```
    MIME type: application/x-java-jnlp-file
    File Extension: jnlp
    ```
  - The HTTP server must be configured and running.
- The system on which you are running the browser (the client) requires the following:
  - The Java Runtime Environment (JRE) 5.0 or later must be installed. Below are the specific requirements:
    - Sun 32-bit JRE 5.0 or later for Intel based systems (x86 and IA64)
    - IBM 64-bit JRE 5.0 or later for PowerPC
    - Sun 32-bit JRE 5.0 or later x86-64

  Refer to the appropriate vendor documentation for detailed instructions about configuring MIME types, configuring and starting the HTTP server and installing the JRE.
- The HBAnyware utility must be installed before installing HBAnyware with Web Launch.

Procedure

To install HBAnyware with Web Launch:

1. Log on as ‘root’.
2. Navigate to the HBAnyware directory. Type:

   ```
   cd /usr/sbin/hbanyware
   ```
3. Run the install script. Type:

   ```
   ./wsinstall
   ```
4. When prompted, enter the Web server's document root directory. For example:

   ```
   /srv/www/htdocs
   ```
5. You are provided with the IP address of the host and asked if that is the IP address that is being used by your Web server. Answer Y or N as appropriate. If you answer N, you are prompted for the IP address you wish to use.
6. You are asked if your web server listening on the normal default HTTP port (80)? Answer Y or N as appropriate. If you answer N, you are prompted for the port you wish to use.

   You are notified the installation of the HBAnyware Web Launch package has completed.

Installing the HBAnyware Security Configurator

Follow these instructions to install the HBAnyware Security Configurator on your system. The install script is located in the /usr/sbin/hbanyware directory.

Prerequisites

- The lpfc driver must be installed.
- The HBAnyware utility must be installed on all participating systems.

Procedure

To install the HBAnyware Security Configurator utility:

1. Log on as ‘root’.
2. Change (use the cd command) to the directory to which you copied the tar file. (See “Installing the Applications Kit” on page 7 step 2 for reference.)
3. Run the install script with the "ssc" parameter specified. Type:

   ```
   ./install ssc
   ```

Uninstalling the Driver Kit

Note: Driver parameter changes made using the HBAnyware utility or /etc/modprobe.conf persist if the driver is uninstalled. To return to the default settings, you must modify the settings in /etc/modprobe.conf.

Note: You must run the uninstall script that shipped with the version of the driver kit you want to remove.

This section describes how to uninstall a previous version of the Emulex 8.x driver for Linux. The uninstall procedure automatically restores the archived lpfc driver.

To uninstall the lpfc driver:

1. Log on as 'root'.
2. If possible, exit all applications that use Fibre Channel-attached drives, then unmount the drives. If you cannot exit all applications that use Fibre Channel-attached drives, the uninstall will work properly, but you must reboot after the uninstallation is complete.
3. Stop the HBAnyware utility. Type:

   ```
   cd /usr/sbin/hbanyware
   ./stop_hbanyware
   ```
4. Uninstall the Applications Kit. See page 11 for instructions.
5. Copy the lpfc-install script to the temporary directory. For example:

   ```
   cp /usr/src/lpfc/lpfc-install /tmp
   ```
6. Execute the lpfc-install script. with the '--uninstall' option. Type:

   ```
   /tmp/lpfc-install --uninstall
   ```

Uninstalling the Applications Kit

Follow these instructions to uninstall the HBAnyware and lputil utilities and their associated files.

Note: If the HBAnyware Security Configurator is installed, it must be uninstalled before uninstalling the HBAnyware and lputil utilities.

Uninstalling the HBAnyware Security Configurator

Note: You must run the uninstall script that shipped with the version of HBAnyware Security Configurator you want to remove.

To uninstall the HBAnyware Security Configurator:

1. Log on as ‘root’.
2. Change (use cd command) to the directory to which you copied the tar file during installation.
3. Run the uninstall script with the ssc parameter specified. Type:

   ```
   ./uninstall ssc
   ```

Uninstalling HBAnyware with Web Launch

Note: If you installed HBAnyware with Web Launch, you must uninstall it before uninstalling HBAnyware.

To uninstall HBAnyware with Web Launch:

1. Log on as ‘root’.
2. Execute the following script:

   ```
   /usr/sbin/hbanyware/wsuninstall
   ```

This script stops the HBAnyware Web Launch Service daemons (if they are running) and removes all Web Launch related files from the host.

Uninstalling HBAnyware and lputil

Note: You must run the uninstall script that shipped with the version of the HBAnyware and lputil utilities that you want to remove.

Note: If you installed HBAnyware with Web Launch, you must uninstall it before uninstalling HBAnyware.

To uninstall the HBAnyware and lputil utilities and the Application Helper Module:

1. Log on as ‘root’.
2. Change (use cd command) to the directory to which you copied the tar file during installation.
3. Uninstall any previously installed versions. Type:

   ```
   ./uninstall
   ```

Configuration

Introduction

The Emulex driver for Linux has many options that you can modify to provide for different behavior. You can change these options using the HBAnyware® utility (HBAnyware) or the LightPulse® diagnostic utility (lputil). The HBAnyware utility is client/server based and provides 'remote' configuration capability to other host platforms running the HBAnyware utility. This remote configuration capability can be provided either "in-band" (host systems on the same FC SAN) or "out-of-band" (from IP addresses of remote machines). The HBAnyware utility also enables the local and “in-band” discovery of Emulex and OEM branded Emulex HBAs.

The new HBAnyware Web Launch feature enables you to download and launch the HBAnyware user interface by specifying the URL of a server that is hosting the HBAnyware Web Launch software. The client machine from which the request is being made does not need the HBAnyware package or even an installed Emulex HBA. You only need a standard web browser, or some other application capable of making HTTP requests. You do not even need the Java runtime as that too will be automatically downloaded if it is not already present.

Note: Only the HBAnyware Web Launch GUI is being exported to the requesting client. All HBA discovery and remote management operations are performed by resources running on the remote host that served up the GUI component. Therefore, the SAN "view" displayed by the GUI is not from the perspective of the client running the GUI, but rather from the perspective of the host from which this GUI was retrieved.

Note: The Linux 2.6 SCSI midlayer provides a number of additional services compared to earlier Linux 2.4 kernels. For an overview of 2.6 SCSI and Emulex driver changes, see the white paper on the Linux section of the Emulex Web site.

- The HBAnyware utility is a user-friendly graphical environment. Use the HBAnyware utility to do any of the following:
    - Discover local and remote hosts, host bus adapters (HBAs), targets and LUNs
    - Enables the local and “in-band” discovery of Emulex and OEM branded Emulex HBAs
    - Reset HBAs
    - Set HBA driver parameters
    - Set driver parameters simultaneously to multiple HBAs using Batch Update
    - Set global driver parameters to HBAs
    - Update firmware on a single HBA or multiple HBAs using Batch Update
    - Enable or disable the BIOS
    - Run diagnostic tests on HBAs
    - Manage out-of-band HBAs
    - Manage local and in-band remote HBAs
    - Locate HBAs using beaconing
    - Launch HBAnyware directly from your Web browser

- The lputil utility is a console application. The lputil utility can be used as an alternative to the HBAnyware utility to do any of the following:
    - List HBAs
    - View HBA information
    - Reset HBAs
    - Update firmware on the local HBA
    - Load EFIBoot
    - Enable the HBA BIOS
    - Download PCI configuration data files

Note: Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

Starting the HBAnyware Utility for Linux

Note: The HBAnyware utility can only discover and manage remote HBAs on hosts running the HBAnyware utility's elxhbamgr daemon.

Starting the HBAnyware Utility

Note: For in-band management, remote capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone.

To start the HBAnyware utility:

1. su to 'root'.
2. Run the script:

   `/usr/sbin/hbanyware/hbanyware`

Starting the HBAnyware utility with Web Launch

After the HBAnyware Web Launch software has been installed and the Web Launch server has been initialized, you can launch the HBAnyware utility directly with your Web browser.

To launch the HBAnyware utility with your Web browser:

1. Open your Web browser.
2. Enter the URL of an HBAnyware.jnlp file. Make sure that the URL specifies a remote server which has the HBAnyware Web Launch software installed and running. For example:

   `http://138.239.20.30/hbanyware.jnlp`

   Note: If the browser window displays "Emulex Corporation HBAnyware Demo of HBAnyware WebStart web n.n.n.n ..." when attempting to start HBAnyware with Web Launch, refer to the "Troubleshooting" section on page 101.

Starting the HBAnyware Security Configurator

Prerequisites

- Make sure that all of the systems that are part of, or will be part of, the security configuration are online on the network so that they receive updates or changes made to the security configuration.
- Before running the security configurator out-of-band, you must setup the OOB hosts or they will not be seen by the security configurator. See the Out-of-Band SAN Management topics for information.

Procedure

To start the HBAnyware Security Configurator:

1. su to ‘root’.
2. Change to the application installation directory. Type:

   ```
   ./install ssc
   ```
3. Run the script:

   ```
   /usr/sbin/hbanyware/ssc
   ```

Starting the HBAnyware Utility from the Command Line

To launch the HBAnyware utility from the command line:

1. Type /usr/sbin/hbanyware/hbanyware. This starts the HBAnyware utility running in in-band access. You can also start the HBAnyware utility running in out-of-band access by adding an argument in the form “h=<host>”. The <host> argument may be either the IP address of the host or its system name. The call will use a default IP port of 23333, but you can override this by optionally appending a colon (:) and the IP port number.

   Note: Remember that not all HBAs for a specific host may be running in-band. Therefore, running that host out-of-band may display HBAs that do not appear when the host is running in-band.

Examples of Modifications

- ./hbanyware h=138.239.82.2

  The HBAnyware utility will show HBAs in the host with the IP address 138.239.82.2.
- ./hbanyware h=Util01

  The HBAnyware utility will show HBAs in the host named Util01.
- ./hbanyware h=138.239.82.2:4295

  The HBAnyware utility will show HBAs in the host with the IP address 138.239.82.2 using IP Port 4295.
- ./hbanyware h=Util01:4295

  The HBAnyware utility will show HBAs in the host named Util01 using IP port 4295.

  Run this modified command line to launch the HBAnyware utility for a single, remote host in local mode.

Changing Management Mode

During installation you selected a management mode, however you can change it if you enabled that option during installation.

The HBAnyware utility enables you to choose three types of host/HBA management:

- Local Mode: HBA's on this platform can be managed by HBAnyware clients on this platform only.
- Managed Mode: HBA's on this platform can be managed by local or remote HBAnyware clients.
- Remote Mode: The same as “Managed Mode”, but HBAnyware clients on this platform can manage local and remote HBA's.

To change HBAnyware management mode:

1. Run the following script:

   ```
   /usr/sbin/hbanyware/set_operating_mode
   ```

2. Choose the management type you want.

The HBAnyware Utility Window Element Definitions

The HBAnyware utility window contains five basic components: the menu bar, the toolbar, the discovery-tree, the property tabs and the status bar.

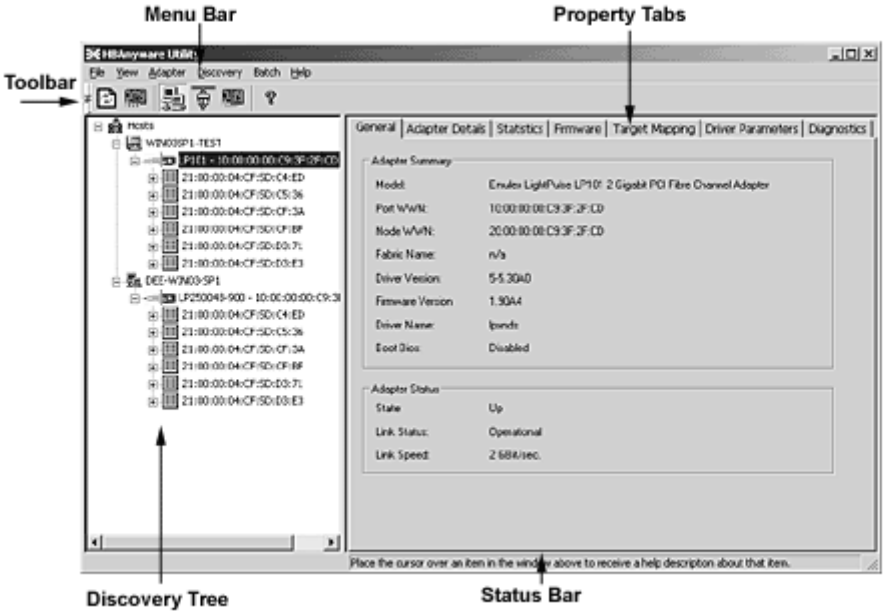


Figure 1: HBAnyware Utility Window with Element Call Outs

Note: The element you select in the discovery-tree determines whether a menu item or toolbar icon is active. For example, if you select the local host or other system host, the Reset Adapter item on the Adapter menu is unavailable. The Reset Adapter toolbar button is unavailable as well.

The Menu Bar

The menu bar contains command menus that enable you to perform a variety of tasks such as exiting the HBAnyware utility, resetting host bus adapters and sorting items in the discovery-tree view. Many of the menu bar commands are also available from the toolbar.

The Toolbar

The toolbar contains buttons that enable you to refresh the discovery-tree, reset the selected HBA and sort the discovery-tree. Many of the toolbar functions are also available from the menu bar.

Figure 2: The HBAnyware Utility Toolbar

The toolbar is visible by default. Use the Toolbar item in the View menu to hide the toolbar. If the item is checked, the toolbar is visible.

The Toolbar Buttons

The toolbar buttons perform the following tasks:

Click the **Rediscover** button to refresh the discovery-tree display.

Click the **Reset** button to reset the selected HBA.

Sort Toolbar Buttons

You can sort discovered adapters by host name or fabric addresses. You can also choose to display only local or remote HBAs. See page 36 for details on sort buttons.

Sort by Host Name button (default)

Sort by Fabric ID button

Local HBAs Only button

Help button

The Discovery-Tree

The discovery-tree (left pane) has icons that represent discovered network (SAN) elements (local host name, system host names and all HBAs active on each host). Targets and LUNs, when present, are also displayed.

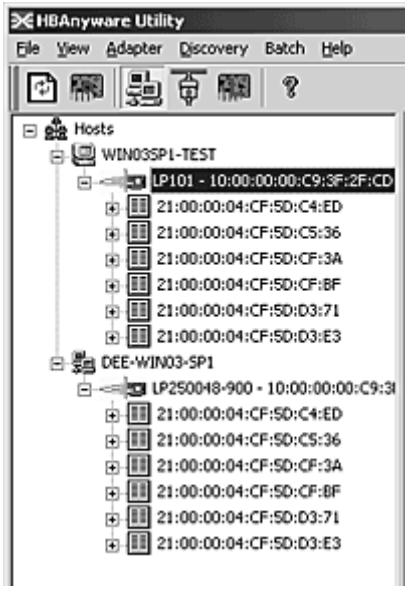


Figure 3: HBAnyware Utility, Discovery-tree

Discovery-Tree Icons

Discovery-tree icons represent the following:

This icon represents the local host.

This icon represents other hosts connected to the system.

A green HBA icon with black descriptive text represents an online HBA.

A red HBA icon with red descriptive text represents an offline or otherwise temporarily inaccessible HBA. Several situations could cause the HBA to be offline or inaccessible:

- The HBA on a local host is not connected to the network, but is still available for local access.
- The HBA on a local host is malfunctioning and is inaccessible to the local host as well as to the network.
- The HBA on a local host is busy performing a local download and is temporarily inaccessible to the local host as well as to the network.

The Target icon represents connections to individual storage devices.

The LUN icon represents connections to individual LUNs.

Property Tabs

The property tabs display configuration, statistical and status information for network elements. The set of available tabs is context-sensitive, depending on the type of network element or HBA currently selected in the discovery-tree.

Status Bar

The status bar is located near the bottom of the HBAnyware utility window. The status bar displays messages about certain HBAnyware utility functions, such as “Discovery in process”.

The status bar is visible by default. Use the Status Bar item in the View menu to hide the status bar. If checked, the status bar is visible.

Using the the HBAnyware Utility Command-Line Interface

The Command Line Interface (CLI) Client component of the HBAnyware utility provides access to the capabilities of the Remote Management library from a console command prompt. This component is intended for use in scripted operations from within shell scripts, batch files, or the specific platform equivalent.

Note: The HBAnyware utility can only discover and manage remote HBAs on hosts running the HBAnyware utility’s elxhbamgr daemon.

Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

Using the CLI Client

The CLI Client is a console application named hbacmd. Each time you run this application from the command line, a single operation is performed.

The first parameter of this command is the requested operation. When the specified operation is completed, the command prompt is displayed. Most operations retrieve information about an entity on the SAN and display that information on the console.

Most of the CLI Client commands require one or more additional parameters that specify the nature of the command. A parameter used by many hbacmd commands specifies the World Wide Port Name (WWPN) of the HBA that is the target of the command. For example, the following command shows the port attributes for the HBA with the specified WWPN:

```
/usr/sbin/hbanyware/hbacmd portattrib 10:00:00:00:c9:20:20:20
```

hbacmd can be run in out-of-band mode by making the first argument h=<host>. For example:

```
/usr/sbin/hbanyware/hbacmd h=cp-hp5670 listhbas
/usr/sbin/hbanyware/hbacmd h=138.239.91.121 listhbas
```

Syntax Rules

The syntax rules for the HBAnyware utility Command-Line Interface (hbacmd) are as follows:

- All commands and their arguments are NOT case sensitive.
- The requested operation must contain at least three characters, or as many as needed to distinguish it from any other operation.
- Whenever a WWPN is specified, individual fields are separated by colons (:) or spaces ( ). When using space separators, the entire WWPN must be enclosed in quotes (").
- All hbacmd inputs must be in hexadecimal format. The only exceptions are the cycle-counts used in some of the diagnostic commands.

Out-of-Band Access

Out-of-band (OOB) access enables you to access HBAs via their IP-address or by the name of the host on which they reside. Since HBAs may exist on a host but not be a part of a FC network, they will not appear during normal in-band discovery. Thus, OOB access enlarges the number of HBAs that can be queried or modified.

Note: A local host cannot be accessed out-of-band.

OOB access via hbacmd uses an additional parameter on the command line. The parameter must be the first parameter in the list, coming immediately after hbacmd. The remaining parameters are those documented for each operation.

Note: You can also access an in-band HBA via its OOB address.

The format of the OOB parameter is:

h={<IPAddress> | <host-name>}

Some examples are:

```
h=128.239.91.88
h=cp-compaq8000
```

The following lists all HBAs running on the host with a specified IP address:

```
hbacmd h=128.239.91.88 listHBAs
```

If you don't know the IP address, but you know the host name, type:

```
hbacmd h=cp-compaq8000 listHBAs
```

If the host is unreachable, the command will return an error.

The CLI Client Command Reference

Note: CLI Client commands are not case sensitive.

Note: The PersistentBinding, SetPersistentBinding, RemovePersistentBinding, RemoveAllPersistentBinding, BindingCapabilities, BindingSupport and SetBindingSupport commands are not supported.

Version

Syntax: HBACMD Version

Description: Shows the current version of the HBAnyware CLI client application. To view the current version, type:

```
hbacmd version
```

Sample response:

```
HBAnyware Command Line Interface: Version 3.2a3
```

Parameters: None.

ListHBAs

Syntax: HBACMD ListHBAs

Description: Shows a list of the discovered manageable Emulex HBAs and some of their attributes. The list will contain one 6-attribute group for each discovered HBA. Example of an attribute group list:

```
Manageable HBA List
Port WWN:    10:00:00:00:c9:20:08:cc
Node WWN:    20:00:00:00:c9:20:08:cc
Fabric Name:10:00:00:60:69:90:0b:f6
Flags:       0000f900
Host Name:   CP-EMULEX-DECPC
Mfg:         Emulex Corporation
```

Parameters: None.

SaveConfig

Syntax: HBACMD SaveConfig <wwpn> <filename> <ctrlword>

Description: Saves the contents of the driver parameter list to a file for the specified HBA. The ASCII file lists parameter definitions, delimited by a comma. Each definition is of the form:

```
<parameter-name>=<parameter-value>
```

Save either the values of the global set or those specific to the referenced HBA. The file created by this command stores itself in the Emulex Repository directory.

Example:

```
hbacmd SaveConfig elxstor-5-1.20A0.dpv 10:00:00:00:c9:2e:51:2e N
```

Sample response:

```
HBACMD_SaveConfig: Success writing driver parameters to file
C:\Program Files\HBAnyware\Emulex Repository\elxstor-5-1.20A.dpv
```

Parameters:

WWPN - The World Wide Port Name of the HBA. This HBA can be either local or remote.

filename - The file name that will contain the driver parameter list upon successful completion of this command.

ctrlword - G = save the global parameter set. N = save the local (HBA-specific) parameter set.

HBAAttrib

Syntax: HBACMD HBAAttrib <wwpn>

Description: Shows a list of all HBA attributes for the HBA with the specified WWPN. To view the attributes for the HBA, type:

```
hbacmd hbaattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
HBA Attributes for 10:00:00:00:c9:4a:c5:90

Host Name       : localhost.localdomain
Manufacturer    : Emulex Corporation
Serial Number   : BG53059073
Model           : LP1150-F4
Model Desc      : Emulex LP1150-F4 4Gb 1port FC: PCI-X2 SFF HBA
Node WWN        : 20 00 00 00 c9 4a c5 90
Node Symname    : Emulex LP1150-F4 FV2.10A5 DV8.0.16.25
HW Version      : 1036406d
Opt ROM Version:
FW Version      : 2.10A5 (J2F2.10A5)
Vender Spec ID : 10DF
Number of Ports: 1
Driver Name     : lpfc
Device ID       : F0D5
HBA Type        : LP1150-F4
Operational FW : SLI-2 Overlay
SLI1 FW         : SLI-1 Overlay 2.10a5
SLI2 FW         : SLI-2 Overlay 2.10a5
IEEE Address    : 00 00 c9 4a c5 90
Boot BIOS       : Disabled
Driver Version : 8.0.16.25; HBAAPI(I) v2.1.c, 02-02-06
Kernel Version : 1.11a5
```

Parameters:

WWPN - The World Wide Port Name of the HBA. This HBA can be either local or remote.

PortAttrib

Syntax: HBACMD PortAttrib <wwpn>

Description: Shows a list of all port attributes for the port with the specified WWPN. To view the port attributes for the HBA, type:

```
hbacmd portattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Port Attributes for 10:00:00:00:c9:4a:c5:90

Node WWN            : 20 00 00 00 c9 4a c5 90
```

```
Port WWN             : 10 00 00 00 c9 4a c5 90
Port Symname         :
Port FCID            : 11400
Port Type            : Fabric
Port State           : Operational
Port Service Type    : 12
Port Supported FC4   : 00 00 01 20 00 00 00 01
                       00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00
Port Active FC4      : 00 00 01 00 00 00 00 01
                       00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00
Port Supported Speed: Unknown
Port Speed           : 2 GBit/sec.
Max Frame Size       : 2048
OS Device Name       : /sys/class/scsi_host/host10
Num Discovered Ports: 3
Fabric Name          : 10 00 00 60 69 50 15 25
```

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

PortStat

Syntax: HBACMD PortStat <wwpn>

Description: Shows all port statistics for the HBA with the specified WWPN. To view port statistics for the HBA, type:

```
hbacmd portstat 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Port Statistics for 10:00:00:00:c9:20:08:cc

Exchange Count           :  1496534
Responder Exchange Count:  37505
TX Seq Count             :  1588007
RX Seq Count             :  1561255
TX Frame Count           :  1588695
RX Frame Count           :  1561892
TX Word Count            :  19821312
RX Word Count            :  66368000
TX KB Count              :  77427
RX KB Count              :  259250
LIP Count                :  1
NOS Count                :  n/a
Error Frame Count        :  0
Dumped Frame Count       :  n/a
Link Failure Count       :  0
Loss of Sync Count       :  9
Loss of Signal Count     :  0
Prim Seq Prot Err Count  :  0
Invalid TX Word Count    :  0
nvalid RX Frame CRC Cnt  :  0
Link Transition Count    :  0
Active RPI Count         :  0
Active XRI Count         :  0
```

```
Rx Port Busy Count      :  0
Rx Fabric Busy Count    :  0
Primary Sequence Timeout:  0
Elastic Buffer Overrun  :  0
Arbitration Timout      :  0
```

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

ServerAttrib

Syntax: HBACMD ServerAttrib <WWPN>

Description: Shows a list of attributes of the server running locally to the specified HBA. To view the server attributes for the HBA, type:

```
hbacmd serverattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Server Attributes for 10:00:00:00:c9:4a:c5:90

Host Name       : localhost.localdomain
FW Resource Path: /usr/sbin/hbanyware/RMRepository/
DR Resource Path: /usr/sbin/hbanyware/RMRepository/
HBAnyware Server Version: 3.0
```

Parameters:

WWPN - The World Wide Port Name of any HBA local to the designated server. The HBA itself can be either local or remote.

TargetMapping

Syntax: HBACMD TargetMapping <wwpm>

Description: Shows a list of mapped targets and the LUNs attached to each for the port with the specified WWPN. To view the target mapping for 10:00:00:00:c9:20:08:0c, type:

```
hbacmd targetmapping 10:00:00:00:c9:20:08:0c
```

Sample response:

```
Target Mapping for 10:00:00:00:c9:4a:c5:90

FCP ID          : 115E2
SCSI Bus Number: 0
SCSI Target Num: 0
Node WWN        : 50:00:60:E8:02:78:6E:03
Port WWN        : 50:00:60:E8:02:78:6E:03
Tgt Device Name: /dev/sdb

FCP LUN 00      : 0000 0000 0000 0000
SCSI OS Lun     : 0
Lun Device Name: /dev/sdb
Vendor ID       : HITACHI
Product ID      : OPEN-3
Product Version: 0118
SCSI Capacity   : 2347 MB
Block Size      : 512 Bytes

FCP LUN 01      : 0001 0000 0000 0000
```

```
SCSI OS Lun    : 1
Lun Device Name: /dev/sdb
Vendor ID      : HITACHI
Product ID     : OPEN-3
Product Version: 0118
SCSI Capacity  : 2347 MB
Block Size     : 512 Bytes

FCP LUN 02     : 0002 0000 0000 0000
SCSI OS Lun    : 2
Lun Device Name: /dev/sdb
Vendor ID      : HITACHI
Product ID     : OPEN-3
Product Version: 0118
SCSI Capacity  : 2347 MB
Block Size     : 512 Bytes
```

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

Reset

Syntax: HBACMD Reset <wwpn>

Description: Resets the HBA with the specified WWPN. Resetting an HBA may require several seconds to complete, especially for remote devices. This command will return for additional input only after the reset has finished. To reset an HBA whose WWPN is 10:00:00:00:c9:e:51:2e, type:

```
hbacmd reset 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Reset HBA 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

Download

Syntax: HBACMD Download <wwpn> <filename>

Description: Loads the specified firmware image to the HBA with the specified WWPN. To load the firmware image located in hdc190a4.dwc to an HBA with WWPN 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd download 10:00:00:00:c9:2e:51:2e hdc190a4.dwc
```

Sample response for a successful download:

```
Downloading hdc190a4.dwc to hba 10:00:00:00:c9:2e:51:2e
Download Complete.
```

Parameters:

WWPN - The World Wide Port Name of the HBA that is the target of the firmware download. This HBA can be either local or remote.

FileName - The file name of the firmware image you want to load. This can be any file accessible to the CLI client application.

AllNodeInfo

Syntax: HBACMD AllNodeInfo <wwpn>

Description: Shows target node information for each target accessible from the specified HBA. To view the target node data for 10:00:00:00:c9:20:0d:36, type:

```
Hbacmd allnodeinfo 10:00:00:00:c9:20:0d:36
```

Sample response:

```
All Node Info for 10:00:00:00:c9:4a:c5:90

Node Type       : EXIST
FCP ID          : 115E2
SCSI Bus Number: 0
SCSI Target Num: 0
Node WWN        : 50:00:60:E8:02:78:6E:03
Port WWN        : 50:00:60:E8:02:78:6E:03
OS Device Name : /sys/class/scsi_host/host10/device/target10:0:0
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose target node information you want to query. This HBA can be either local or remote.

DriverConfig

Syntax: HBACMD driverconfig <wwpn> <filename><ctrlword>

Description: Sets all driver parameters for the HBA specified by WWPN to the driver parameter values contained in the driver parameter file. These files can be easily generated via the HBAnyware Driver Parameter tab. Driver types must match between .dpv file type and host platform HBA.

For example, type:

```
hbacmd driverconfig 10:00:00:00:c9:2e:51:2e elxconfig G
```

Below is a sample response:

hbacmd: Success setting driver configuration parameters to values in .dpv file.

Parameters:

WWPN - The World Wide Port Name of the HBA on which to set driver parameters.

ctrlword - G = save the global parameter set. N = make change neither permanent nor global.

GetDriverParams

Syntax: HBACMD GetDriverParams <wwpn>

Description: Shows the name and values of each driver parameter for the selected HBA. To view the driver parameters for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd getdriverparams 10:00:00:00:c9:2e:51:2e
```

Sample (abbreviated) response:

```
Driver Params for 10:00:00:00:c9:4a:c5:90. Values in HEX format.
```

DX	string	Low	High	Def	Cur	Exp	Dyn
00	log-verbose	0	ffff	0	20	1	1
01	lun-queue-depth	1	80	1e	1e	1	4
02	scan-down	0	1	1	1	1	4

03	nodev-tmo	0	ff	1e	3c	1	1
04	topology	0	6	0	0	1	4
05	link-speed	0	4	0	0	1	4
06	fcp-class	2	3	3	3	1	4
07	use-adisc	0	1	0	1	1	1
08	ack0	0	1	0	0	1	4
09	fcp-bind-method	1	4	2	2	1	4
0a	cr-delay	0	3f	0	0	1	4
0b	cr-count	1	ff	1	1	1	4
0c	fdmi-on	0	2	0	0	1	4
0d	discovery-threads	1	40	20	20	1	4
0e	max-luns	1	8000	100	100	1	4

Parameters:

WWPN - The World Wide Port Name of the HBA whose driver parameters you want to view. This HBA can be either local or remote.

GetParamsGlobal

Syntax: HBACMD GetParamsGlobal <wwpn>

Description: Shows the name and the global value of each driver parameter for the selected HBA. To view the global driver parameters for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd getparamsglobal 10:00:00:00:c9:2e:51:2e
```

Sample (abbreviated) response:

```
Driver Params (Global) for 10:00:00:00:c9:2e:51:2e. Values in HEX.
```

DX	string	Low	High	glbl	Cur	Exp	Dyn
00	log-verbose	0	ffff	0	40	1	1
01	lun-queue-depth	1	80	1e	1e	1	4
02	scan-down	0	1	1	1	1	4
03	nodev-tmo	0	ff	1e	1e	1	1
04	topology	0	6	0	0	1	4
05	link-speed	0	4	0	0	1	4
06	fcp-class	2	3	3	3	1	4
07	use-adisc	0	1	0	0	1	1
08	ack0	0	1	0	0	1	4
09	cr-delay	0	3f	0	0	1	4
0a	cr-count	1	ff	1	1	1	4
0b	fdmi-on	0	2	0	0	1	4
0c	discovery-threads	1	40	20	20	1	4
0d	max-luns	1	8000	100	100	1	4

Parameters:

WWPN - The World Wide Port Name of the HBA whose driver parameters you want to view. This HBA can be either local or remote.

SetDriverParam

Note: This command may only be used with the lpfc_log_verbose, lpfc_use_adisc and lpfc_nodev_tmo parameters.

Syntax: HBACMD SetDriverParam <wwpn> <cw1> <cw2><param> <value>

Description: Changes the value of the specified driver parameter that is operating the referenced HBA, and designates the scope of that change. For example, to change the value of the log_verbose parameter for 10:00:00:00:c9:2e:51:2e and make it global, type:

```
hbacmd SetDriverParam 10:00:00:00:c9:2e:51:2e g log_verbose 3
```

Sample response:

```
Set Driver Parameter log_verbose=3(g) for 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose Boot BIOS you want to modify. This HBA can be either local or remote.

cw1 - L = Local, for this adapter only. G = Global, all adapters on this host.

cw2 - P = Permanent, persists across reboots. T = Temporary, lost after reboot.

param - The name of the parameter whose value you want to modify. You can only use the log_verbose, use_adisc and _nodev_tmo parameters. Do not preceed these commands with lpfc_. For example use log_verbose not lpfc_log_verbose.

Value - The new value you want to assign to the parameter. Prefix with 0x to input as hexidecimal.

SetDriverParamDefaults

Note: This command may only be used with the lpfc_log_verbose, lpfc_use_adisc and lpfc_nodev_tmo parameters.

Syntax: HBACMD SetDriverParamDefaults <wwpn> <cw1> <cw2>

Description: Returns the driver settings to their default parameters.

Parameters:

WWPN - The World Wide Port Name of the HBA whose Boot BIOS you want to modify. This HBA can be either local or remote.

cw1 - L = Local, for this adapter only. G = Global, all adapters on this host.

cw2 - P = Permanent, persists across reboots. T = Temporary, lost after reboot.

SetBootBios

Syntax: HBACMD SetBootBios <wwpn> <ctrlword>

Description: Enables or disables the BootBIOS on the referenced HBA. To enable the BootBIOS for 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd setbootbios 10:00:00:00:c9:2e:51:2e E
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose BootBIOS you want to modify. This HBA can be either local or remote.

ctrlword - E = enable the Boot BIOS, D = disable the BootBIOS.

PciData

Syntax: HBACMD PciData <wwpn>

Description: Shows PCI configuration data for the HBA specified by the WWPN. To show PCI configuration data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd pcidata 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Vendor ID:            0x10DF       Device ID:            0xF0D5
Command:              0x0157       Status:               0x0230
Revision ID:          0x01         Prog If:              0x00
Subclass:             0x04         Base Class:           0x0C
Cache Line Size:      0x20         Latency Timer:        0xF8
Header Type:          0x00         Built In Self Test:   0x00
Base Address 0:       0xE0001004   Base Address 1:
0x00000000
Base Address 2:       0xE0000004   Base Address 3:
0x00000000
Base Address 4:       0x0000C001   Base Address 5:
0x00000000
CIS:                  0x00000000   SubVendor ID:         0x10DF
SubSystem ID:        0xF0D5       ROM Base Address:    0x00000000
Interrupt Line:       0xFF         Interrupt Pin:        0x01
Minimum Grant:        0xFF         Maximum Latency:      0x00
Capabilities Ptr:     0x5C
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose PCI configuration data you want to show.

Wakeup

Syntax: HBACMD wakeup <wwpn>

Description: Shows wakeup parameter data for the HBA specified by the WWPN. To show wakeup parameter data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd wakeup 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Wakeup Parameters:
Initial Load:          0x02C03992        0x00103411
```

Flags:	0x00000000	
Boot BIOS	0x03433290	0x00101303
SLI-1:	0x06433992	0x00103411
SLI-2:	0x07433992	0x00103411
Has Expansion ROM	0	

Parameters:

WWPN - The World Wide Port Name of the HBA whose wakeup parameter data you want to show.

LoopMap

Syntax: HBACMD loopmap <wwpn>

Description: Shows the arbitrated loop map data for the HBA specified by the WWPN. To show the arbitrated loop map data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd loopmap 10:00:00:00:c9:2e:51:2e
```

Below is a sample response:

```
AL_PA:
01 Local Adapter
E8 SCSI Device
E4 SCSI Device
CA SCSI Device
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose loopmap you want to show.

GetBeacon

Syntax: HBACMD getbeacon <wwpn>

Description: Shows the current beacon status for the HBA specified by the WWPN. To show the current beacon status for HBA 10:00:00:00:c9:2e:51:2e, type:

For example, type:

```
hbacmd getbeacon 10:00:00:00:c9:2e:51:2e
```

Possible responses are:

```
Beacon State = On
Beacon State = Off
Unable to get Beacon state, error 1
 not supported on host or adapter
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose beacon status you want to show.

SetBeacon

Syntax: HBACMD setbeacon <wwpn> <state>

Description: Sets the current beacon status for the HBA specified by the WWPN. To set the current beacon status for HBA 10:00:00:00:c9:2e:51:2e to off, type:

```
hbacmd setbeacon 10:00:00:00:c9:2e:51:2e 0
```

To set the current beacon status for HBA 10:00:00:00:c9:2e:51:2e to on, type:

```
hbacmd setbeacon 10:00:00:00:c9:2e:51:2e 1
```

Possible responses are:

```
Beacon State successfully set to On
Beacons State successfully set to Off
Unable to get Beacon state, error 1
Beaconing not supported on host or adapter
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose beacon status you want to set. This HBA can be either local or remote.

State - The new state of the beacon: 0 = beacon OFF, 1= beacon ON

PostTest

Syntax: HBACMD posttest <wwpn>

Description: Runs the POST test on the HBA specified by the WWPN. Support for remote HBA is out-of-band (Ethernet) only. To run the POST test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd posttest 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Running POST, polling for results.....
Power On Self Test Succeeded;time to execute = 8928 ms
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to run the POST test.

EchoTest

Syntax: HBACMD echotest <wwpn1> <wwpn2> <count> <StopOnError>

Description: Runs the echo test on the HBAs specified by the WWPN1 and WWPN2.

Note: Support for remote HBA is out-of-band (Ethernet) only. The EchoTest command will fail if the target WWPN does not support the ECHO ELS command.

To run the echo test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd echotest 10:00:00:00:c9:2e:51:2e
10:00:00:00:c9:2e:51:45 10 1
```

Sample response:

```
Echo test: polling for results......
Echo test succeeded; time to execute = 53 ms.
```

Parameters:

WWPN1 - The World Wide Port Name of the originating HBA.

WWPN2 - The World Wide Port Name of the destination (echoing) HBA.

Count - The number of times to run the test.

StopOnError - Should the test be halted on Error? 0 = no halt, 1 = halt

Loopback

Syntax: HBACMD loopback <wwpn> <type> <count> <StopOnError>

Description: Runs the loop test on the HBA specified by the WWPN.

Note: Only external Loopback tests must be run out-of-band.

To run the loop test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd loopback 10:00:00:00:c9:2e:51:2e 1 10 0
```

Sample response:

```
Running Loopback:  polling for results......
Loopback Test Failed; xmit errors = 3; rcv errors = 2; time to
execute = 1015 ms.
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to run the loopback test(s).

Type - Type of loopback test where: 0 = PCI LoopBack Test, 1 = Internal LoopBack Test, 2 = External LoopBack Test

Count - The number of times to run the test (Range = 1,...10000).

StopOnError - Should the test be halted on Error? 0 = no halt, 1 = halt

Dump

Syntax: HBACMD dump <wwpn>

Description: Runs the dump diagnostic retrieval command on the HBA specified by the WWPN. This command is supported for local HBAs only. The file by default is located in:
/usr/sbin/hbanyware/Dump

To run the dump diagnostic retrieval command for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd dump 10:00:00:00:c9:2e:51:2e
```

Sample response (Abbreviated list):

```
Revision Information: OS Version
 Linux, 2.6.16.20-0.12-smp

Revision Information: Driver Version
 Driver Type: Linux lpfc
 Driver Name: lpfc
 Driver Version: 8.1.6.2; HBAAPI(I) v2.1.c, 02-02-06

Revision Information: HBAnyware Version
 HBAnyware Version: 3.2a3
 DFC Lib Version:   2.14.0

HBA Information: Adapter Model
 Model: LPe11002-M4
 Description: Emulex LPe11002-M4 4Gb 2port FC: PCIe SFF HBA

HBA Information: Adapter WWN
 Port WWN: 10:00:00:00:c9:4e:2b:28
 Node WWN: 20:00:00:00:c9:4e:2b:28

HBA Information: Adapter Serial Number
 Adapter Serial Number: VM54139218

HBA Information: Firmware Version
 Firmware Version: 2.50A6 (Z2F2.50A6)
 Operational FW Version: SLI-2 Overlay
 SLI-1 FW Version: SLI-1 Overlay 2.50a6
 SLI-2 FW Version: SLI-2 Overlay 2.50a6
 Kernel FW Version: 1.12a6

HBA Information: Boot Bios Version
 Boot Bios State: 0
 Boot Bios Version: Boot Bios Firmware 5.01a7
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to you want to run the dump.

DeleteDumpFiles

Syntax: HBACMD deletedumpfiles <wwpn>

Description: Deletes all dump files associated with the HBA specified by the WWPN. To delete all dump files for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd deletedumpfiles 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
HBACMD: Dump file deletion complete.
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose dump files you want to delete.

Starting the lputil Utility

The LightPulse diagnostic utility (lputil) is installed automatically when the driver utilities kit is installed.

Start the utility by entering the complete path to lputil. The path reflects the default installation path. If the installation path changed, you must adjust the command appropriately.

To start the lputil utility type:

```
/usr/sbin/lpfc/lputil
```

Discovering HBAs

You can discover HBAs using either the HBAnyware or lputil utility.

- The HBAnyware utility allows you to discover both local and remote HBAs.
- The lputil utility allows you to discover only local HBAs.

Discovering HBAs Using the HBAnyware Utility

Local and remote HBAs are discovered automatically when you launch the HBAnyware utility. Initially, both local and remote HBAs are displayed. You can also discover HBAs on out-of-band (OOB) hosts. For more information, see “Out-of-Band Access” on page 19.

Note: The HBAnyware utility must be installed and the elxhbamgr process(es) must be running on all remote hosts that you want to discover and manage.

Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

When an in-band HBA becomes unavailable (as seen by the HBAnyware utility running remotely) the target WWPN changes color from black (normal) to blue and the target information is not removed from the discovery-tree until the undiscovered HBA timer has expired (See Configuring Discovery Settings on page 35). Similarly, when an out-of-band host is no longer seen by the HBAnyware utility, the HBAs on that host will change from black (normal) to blue, and the target information is not removed from the discovery-tree until the undiscovered HBA timer has expired.

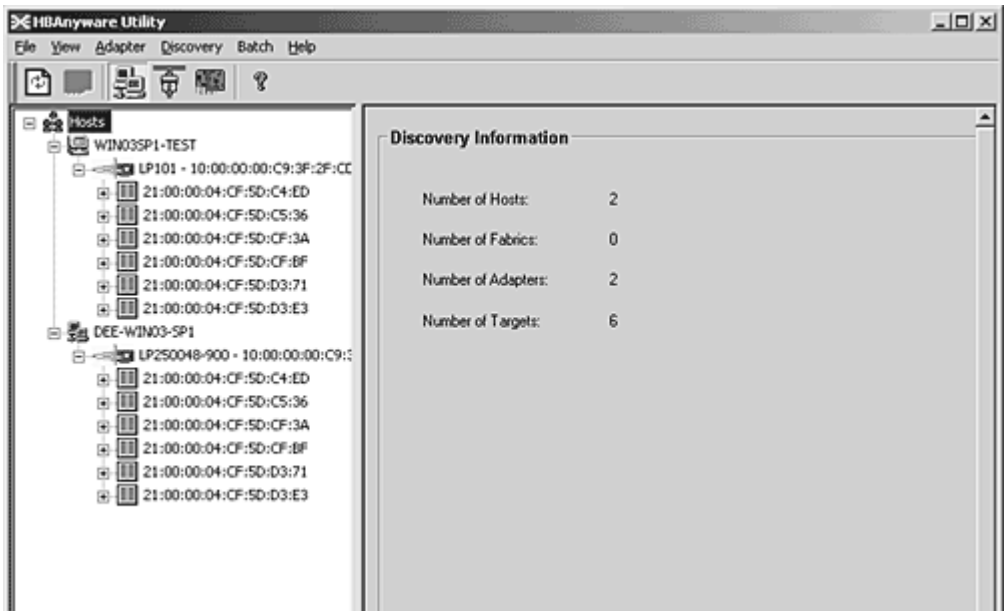


Figure 4: HBAnyware Utility, Discovery Information

Note: Emulex recommends setting the monitor display resolution to 1024x768 as a minimum to properly view the HBAnyware utility.

Configuring Discovery Settings

Use the HBAnyware Discovery Settings dialog box to configure several discovery server parameters. You can define when to start the discovery server, when to refresh in-band and out-of-band discoveries and when to remove previously discovered HBAs that are no longer being discovered.

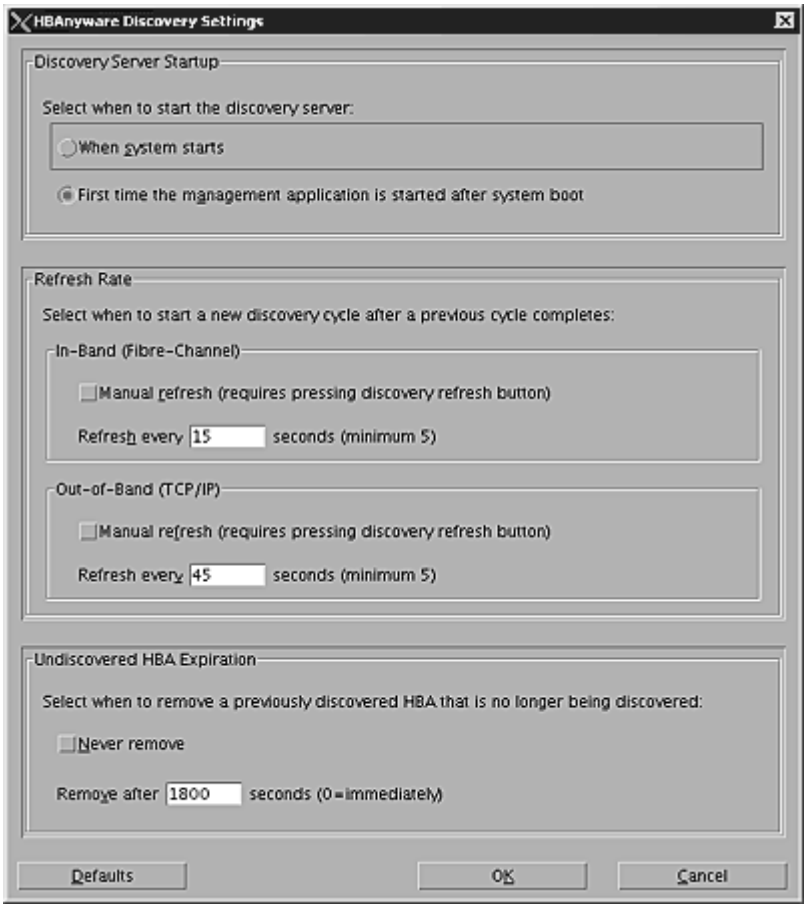

HBAnyware Discovery Settings
Discovery Server Startup
Select when to start the discovery server:
When system starts
First time the management application is started after system boot
Refresh Rate
Select when to start a new discovery cycle after a previous cycle completes:
In-Band (Fibre-Channel)
Manual refresh (requires pressing discovery refresh button)
Refresh every 15 seconds (minimum 5)
Out-of-Band (TCP/IP)
Manual refresh (requires pressing discovery refresh button)
Refresh every 45 seconds (minimum 5)
Undiscovered HBA Expiration
Select when to remove a previously discovered HBA that is no longer being discovered:
Never remove
Remove after 1800 seconds (0=immediately)
Defaults
OK
Cancel

Figure 5: HBAnyware Utility, HBA Discovery Settings Dialog Box

To configure discovery settings:

1. Start the HBAnyware utility.
2. From the Menu bar, select Discovery/Modify Settings. The Discovery Settings dialog box appears.
3. Define the discovery properties you wish and click **OK**. Click **Defaults** to return the discovery properties to their default settings.

Discovering HBAs Using the lputil Utility

When you start the lputil utility, all local HBAs are discovered and listed with information such as the HBA number, instance number (i.e. lpfc0), board model type and whether the HBA is ready to use.

To discover HBAs using the lputil utility:

1. From the Main menu, enter 1, List Adapters.

Figure 6: lputil Utility, Main Menu

Sorting HBA Information

Sorting HBAs Using the HBAnyware Utility

Sort discovered HBAs by host name, fabric name, HBA name, target name and LUN number. You can also choose to view local HBAs or remote HBAs. By default, both local and remote HBAs are sorted by host name/fabric name.

To sort HBAs:

1. Start the HBAnyware utility.
2. Switch between host name or fabric ID in one of two ways:
   - From the menu bar: click **View,** then click **Sort by Host Name** or **Sort by Fabric ID.** The current adapter display mode is checked.
   - From the toolbar, click one of the following buttons:

     Sort HBAs by Host Name (default).

     Sort HBAs by Fabric ID.
3. The HBAnyware utility sorts in ascending order. The sort recognizes letters, numbers, spaces and punctuation marks.

Sort by Host Name

- Initially sorts by host name. You cannot change host names using the HBAnyware utility; names must be changed locally on that system.
- Within each host system, sorts by HBA model.
- If multiple HBAs have the same model number, sorts models by World Wide Node Name (WWNN).

- If targets are present, sorts by World Wide Port Name (WWPN). Multiple HBAs may refer to the same target.
- If LUNs are present, sorts by LUN number.

Sort by Fabric Address

- Initially sorts by fabric ID.
- Within each fabric ID, sorts by HBA model.
- If multiple HBAs have the same model number, sorts models by WWNN.
- If targets are present, sorts by WWPN. Multiple HBAs may refer to the same target.
- If LUNs are present, sorts by LUN number.
- If the fabric ID is all zeros, no fabric is attached.

Sorting Local HBAs Only Using the HBAnyware Utility

Displays local HBA's only. Works in conjunction with the Sort by Host Name and Sort by Fabric ID buttons.

To display local HBAs only, do one of the following:

- From the menu bar: click **View**, then click **Local HBAs Only**. The current adapter display mode is checked.
- From the toolbar, click the **Local HBAs Only** button.

Sorting Local HBAs Using the lputil Utility

Local HBAs are automatically displayed.

Viewing HBA Information Using the HBAnyware Utility

Viewing Discovery Information

The Discovery Information area contains a general summary of the discovered elements. The Host or Fabric icon, depending upon which view you select, is the root of the discovery-tree, but it does not represent a specific network element. Expanding it will reveal all hosts, LUNs, targets and HBAs that are visible on the storage area network (SAN).

To view the discovery information:

1. Start the HBAnyware utility.

2. Click the **Host** or **Fabric** icon at the root of the discovery-tree. Discovered SAN elements appear in the discovery-tree. Select an element from the discovery-tree to learn more about it.

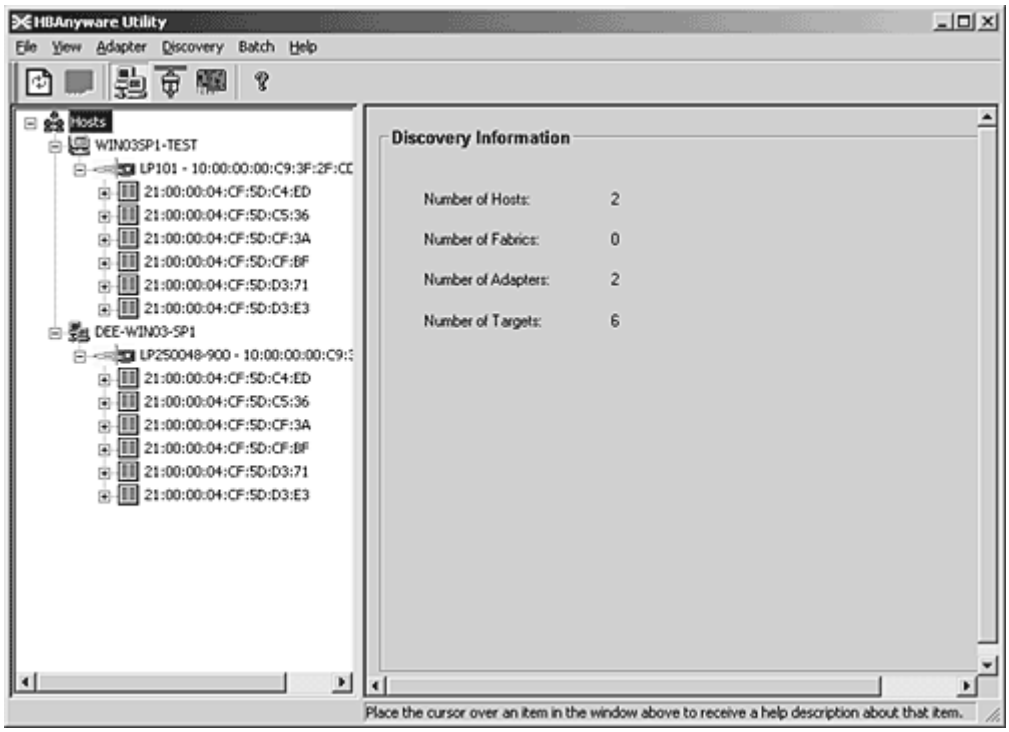


Figure 7: HBAnyware Utility, Discovery Information

Discovery Information Field Definitions

- Number of Hosts - The total number of discovered host computers. This includes servers, workstations, personal computers, multiprocessors and clustered computer complexes.
- Number of Fabrics - The total number of discovered fabrics.
- Number of Adapters - The total number of discovered HBAs.
- Number of Targets - The total number of unique discovered targets on the SAN. In the discovery-tree, the same target can appear under more than one HBA.

Viewing Host Information

There are two tabs that show host information: the Host Information tab and the host Driver Parameters tab. The Host Information tab is read-only. The host Driver Parameters tab enables you to view and define HBA driver settings for a specific host.

To view the Host Information and Driver Parameters tabs:

1. Start the HBAnyware utility.
2. Do one of the following:
   - From the menu bar, click **View**, then click **Sort by Host Name**.
   - From the toolbar, click the **Sort by Host Name** button.
3. Select a host in the discovery-tree.
4. Select the Host Information tab (see Figure 8) or the Host Driver Parameters tab (see Figure 9).

The Host Information Tab

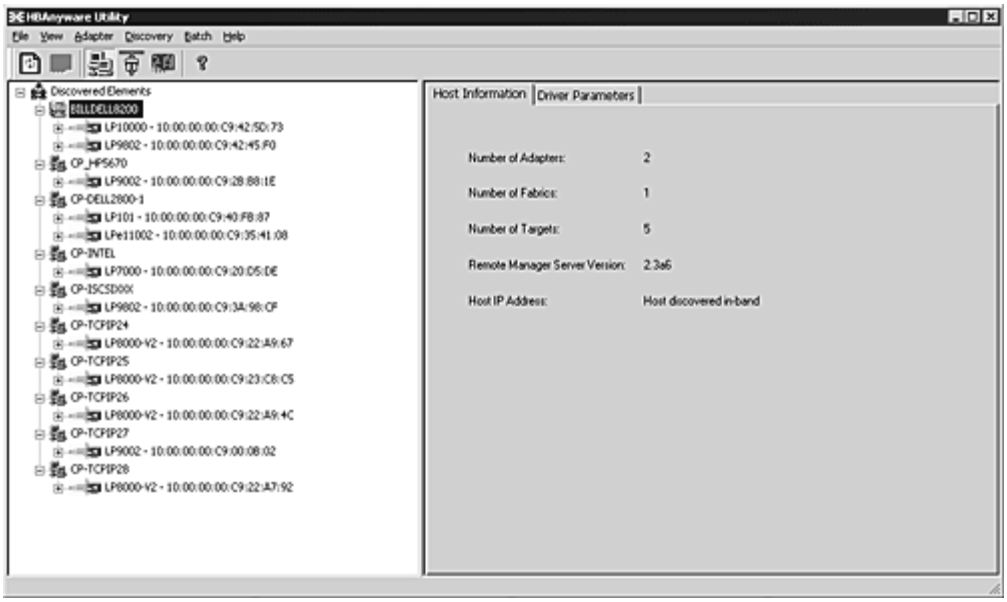


Figure 8: HBAnyware Utility, Host Information Tab

Host Information Field Definitions

- Number of Adapters - The number of HBAs installed in the host.
- Number of Fabrics - The number of fabrics to which this host is attached.
- Number of Targets - The number of storage devices seen by the host.
- Remote Manager Server Version - The version of the the HBAnyware utility server that is running on the host. If different versions of the HBAnyware utility are installed on different hosts in the SAN, those differences appear in this field.
- Host IP Address - If the host is discovered in-band, the dialog box displays "Host discovered in-band." If the host is discovered out-of-band, the dialog box displays the host's IP address, e.g., 138.239.82.131.

The Host Driver Parameters Tab

The Host Driver Parameters tab (Figure 9) enables you to view and edit the HBA driver settings contained in a specific host. The host driver parameters are global values and apply to all HBAs in that host unless they are overridden by parameters assigned to a specific HBA using the HBA Driver Parameters tab. For each parameter, the tab shows the current value, the range of acceptable values, the default value, and whether the parameter is dynamic (a dynamic parameter allows the change to take effect without resetting the HBA or rebooting the system).

Note: For the Linux 2.6 kernal, most driver parameters are set globally. You can set the lpfc_log_verbose, lpfc_nodev_tmo and lpfc_use_adisc locally.

For more information on changing the parameters for a single HBA, see “Setting Driver Parameters for an HBA” on page 60.

For more information changing the parameters for the host, see “Setting Driver Parameters for a Host” on page 62.

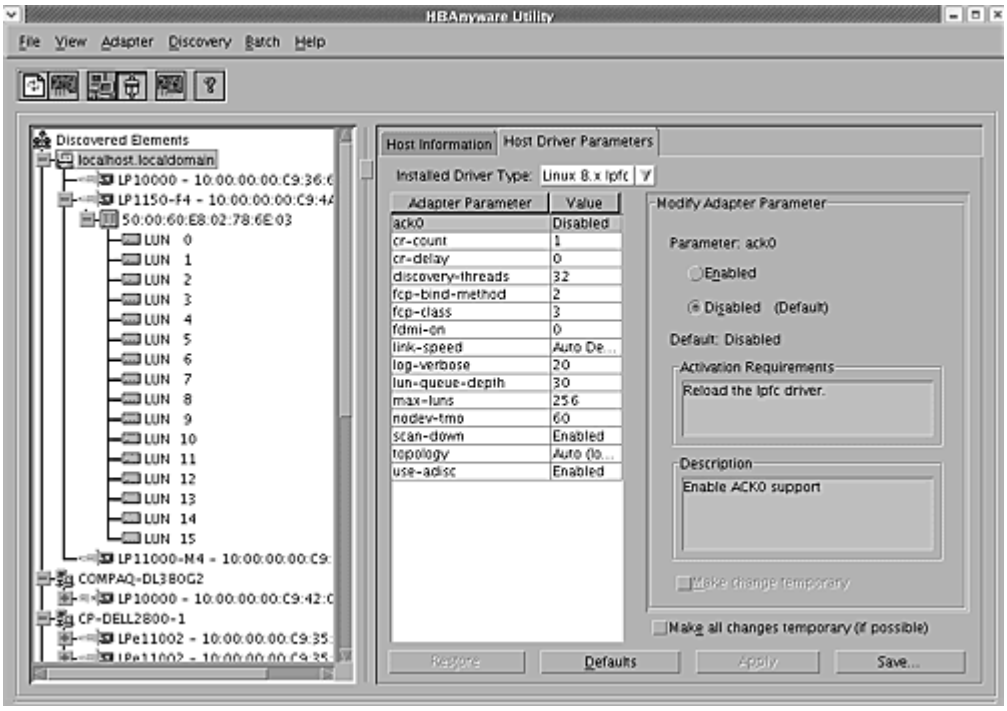


Figure 9: HBAnyware Utility, Driver Parameters Tab - Host Selected

Note: If there is more than one driver type installed, the Installed Driver Types menu shows a list of all driver types and driver versions that are installed on the HBAs in the host.

Driver Parameter Tab Field Definitions

- Installed Driver Type - The current driver and version installed.
- Adapter Parameter table - A list of HBA driver parameters and their current values.
- Parameter-specific information - The details about the parameter appears on the right side of the tab.

Driver Parameter Tab Buttons

- **Restore** - Click to save and restore parameters to this last saved value, if you have made changes to parameters and have not saved them by clicking **Apply**.
- **Defaults** - Click to reset all parameter values to their default (out-of-box) values.
- **Apply** - Click to apply any driver parameter changes. If you changed a parameter that is not dynamic, you must unload the driver and reload it.

Viewing General HBA Attributes

The General tab contains general attributes associated with the selected HBA.

To view general attributes:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.

3. Click an HBA in the discovery-tree.

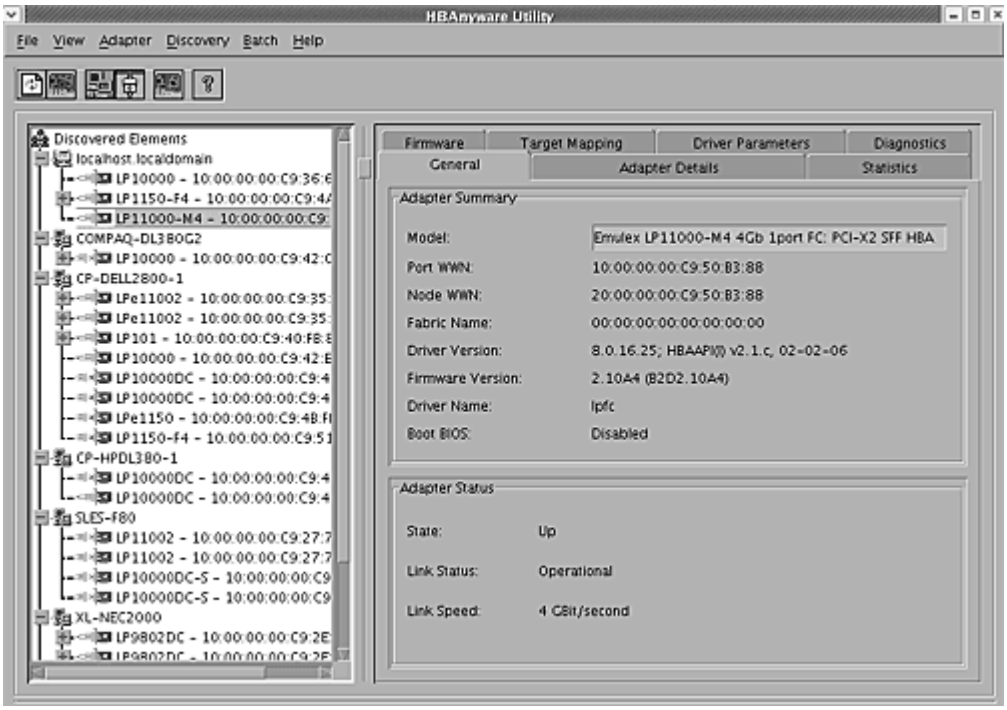


Figure 10: HBAnyware Utility, General Tab

Adapter Summary Field Definitions

- Model - The complete model name of the HBA.
- Port WWN - The Port World Wide Name of the HBA.
- Node WWN - the Node World Wide Name of the selected HBA.
- Fabric Name or Host Name - The Fabric Name field shows if you selected, “Sort by Host Name”. The fabric name is a 64-bit worldwide unique identifier assigned to the fabric. The Host Name field shows if you selected “Sort by Fabric ID”. The host name is the name of the host containing the HBA.
- Driver Version - The version of the driver installed for the HBA.
- Firmware Version - The version of Emulex firmware currently active on the HBA.
- Driver Name - The executable file image name for the driver as it appears in the Emulex driver download package.
- Boot Bios - Indicates if the boot code is enabled or disabled.

Adapter Status Area Field Definitions

State - The current operational state of the HBA: “Up” or “Down”.

Link Status - The current link status between the HBA and the fabric. There are several possible states:

- The “Operational” state indicates that the HBA is connected to the network and operating normally.
- All other states indicate that the HBA is not connected to the network. Green HBA icons with red descriptive text indicate that the HBA is offline. These offline states are:
    - “User offline” - The HBA is down or not connected to the network.

- “Bypassed” - the HBA is in Fibre Channel discovery mode.
- “Diagnostic Mode” - The HBA is controlled by a diagnostic program.
- “Link Down” - There is no access to the network.
- “Port Error” - The HBA is in an unknown state; try resetting it.
- “Loopback” -an FC-1 mode in which information passed to the FC-1 transmitter is shunted directly to the FC-1 Receiver. When a FC interface is in loopback mode, the loopback signal overrides any external signal detected by the receiver.
- “Unknown” -The HBA is offline for an unknown reason.

- Link Speed - The link speed of the HBA in gigabits per second.

Viewing Detailed HBA Information

The Adapter Details tab in the HBAnyware utility contains detailed information associated with the selected HBA.

To view the detailed attributes:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Select an HBA in the discovery-tree.
4. Select the Adapter Details tab.

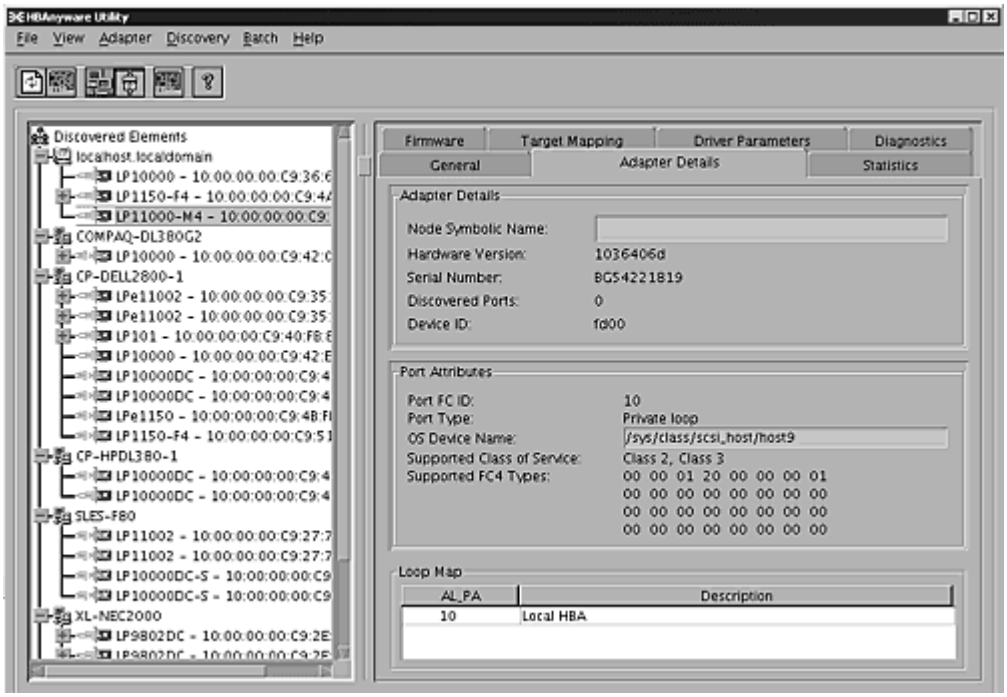


Figure 11: HBAnyware Utility, Adapter Details Tab

Adapter Details Field Definitions

- Node Symbolic Name - The Fibre Channel name used to register the driver with the name server.
- Hardware Version - The JEDEC ID board version of the selected HBA.

- Serial Number - The manufacturer assigned serial number of the selected HBA.
- Discovered Ports - The number of other HBAs visible to the selected HBA.
- Device ID - The HBA's default device ID.

Port Attributes Field Definitions

- Port FC ID - The Fibre Channel ID for the port of the selected HBA.
- Port Type - The current operational mode of the selected HBA's port.
- OS Device Name - The platform-specific name by which the selected HBA is known to the operating system.
- Supported Class of Service - A frame delivery scheme exhibiting a set of delivery characteristics and attributes. There are three classes of service.
    - Class-1 provides a dedicated connection between a pair of ports confirmed with delivery or notification of nondelivery.
    - Class-2 provides a frame switched service with confirmed delivery or notification of non-delivery.
    - Class-3 provides a frame switched service similar to Class-2 but without notification of frame delivery or non-delivery.
- Supported FC4 Types - a 256-bit (8-word) map of the FC-4 protocol types supported by the port containing the selected HBA.

Loop Map Table Definitions

- The loop map shows the different ports present in the loop, and is present only if the port (HBA) is operating in loop mode. The simplest example would be to connect a JBOD directly to an HBA. When this is done, the port type will be a private loop, and the loop map will have an entry for the HBA, and one entry for each of the disks in the JBOD.

Viewing Fabric Information

The Discovery Information area contains information about the selected fabric.

To view the fabric information:

1. Start the HBAnyware utility.
2. Do one of the following:
    - From the menu bar, click **View**, then click **Sort by Fabric ID**.
    - From the toolbar, click the **Sort by Fabric ID** button.

3. Click on a fabric address in the discovery-tree. The Discovery Information tab shows information about the selected fabric.

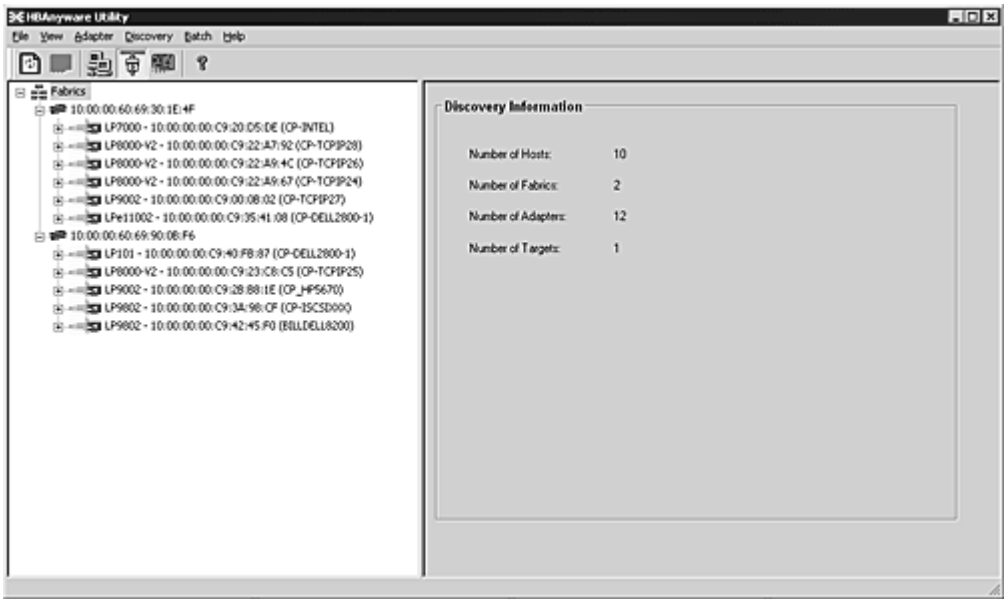


Figure 12: HBAnyware Utility, Discovery Information

Discovery Information Field Definitions

- Number of Hosts - The number of hosts discovered or seen by this host on the selected fabric.
- Number of Fabrics - The number fabrics identified during discovery.
- Number of Adapters - The number of HBAs discovered by this host on the selected fabric.
- Number of Targets - The number of storage devices seen by this host on the selected fabric.

Viewing Target Information

The Target Information area contains information specific to the selected storage device.

To view target information:

1. Start the HBAnyware utility.
2. Do one of the following:

    - From the menu bar, click **View**, then click **Sort by Host Name**.
    - From the toolbar, click the **Sort by Host Name** button.

3. Click a target in the discovery-tree. The Target Information tab appears.

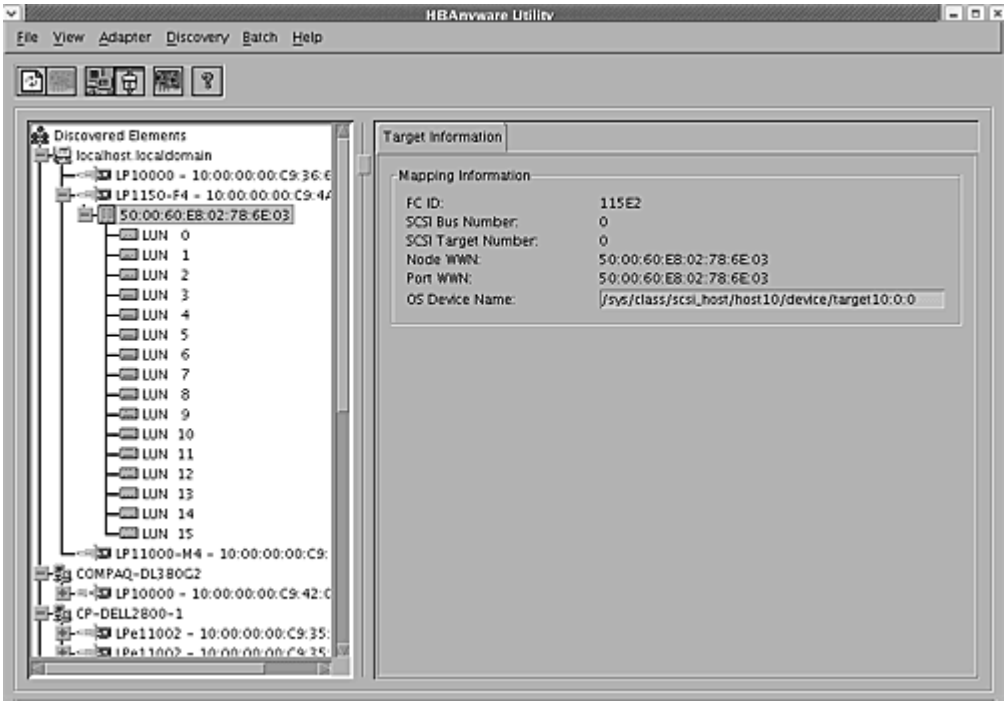


Figure 13: HBAnyware Utility, Target Information

Target Information Field Definitions

- Mapping Information Area
  - FC ID - The Fibre Channel ID for the target; assigned automatically in the firmware.
  - SCSI Bus Number - Defines the SCSI bus to which the target is mapped.
  - SCSI Target Number - The target's identifier on the SCSI bus.
  - Node WWN - A unique 64-bit number, in hexadecimal, for the target (N_PORT or NL_PORT).
  - Port WWN - A unique 64-bit number, in hexadecimal, for the fabric (F_PORT or FL_PORT).
  - OS Device Name - The operating system device name.

Viewing LUN Information

The LUN Information area contains information about the selected logical unit number (LUN).

To view the LUN information:

1. Start the HBAnyware utility.
2. Do one of the following:

   - From the menu bar, click **View**, then click **Sort by Host Name**.
   - From the toolbar, click the **Sort by Host Name** button.

3. Click on a LUN in the discovery-tree.

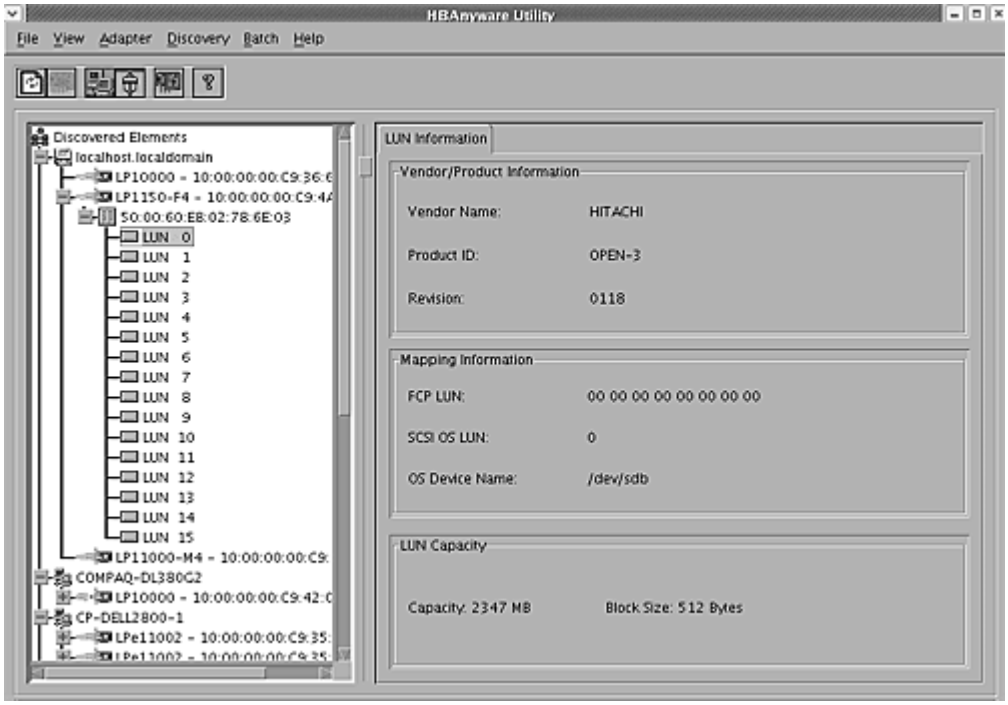


Figure 14: HBAnyware Utility, LUN Information

LUN Information Field Definitions

- Vendor Product Information Area
  - Vendor ID - The name of the vendor of the LUN.
  - Product ID - The vendor-specific ID for the LUN.
  - Revision - The vendor-specific revision number for the LUN.
- Mapping Information Area
  - FCP LUN - The Fibre Channel identifier used by the HBA to map to the SCSI OS LUN.
  - SCSI OS LUN - The SCSI identifier used by the operating system to map to the specific LUN.
  - OS Device Name - The name assigned by the operating system to the selected LUN.
- LUN Capacity

Note: LUN capacity information is only provided when the LUN is a mass-storage (disk) device. Other devices like tapes and scanners, etc. do not display capacity.

  - Capacity - The capacity of the LUN, in megabytes.
  - Block Length - The length of a logical unit block in bytes.

Viewing Port Statistics

The Statistics tab provides cumulative totals for various error events and statistics on the port. Some statistics are cleared when the HBA is reset.

To view port statistics:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Click an HBA in the discovery-tree.
4. Click the **Statistics** tab.

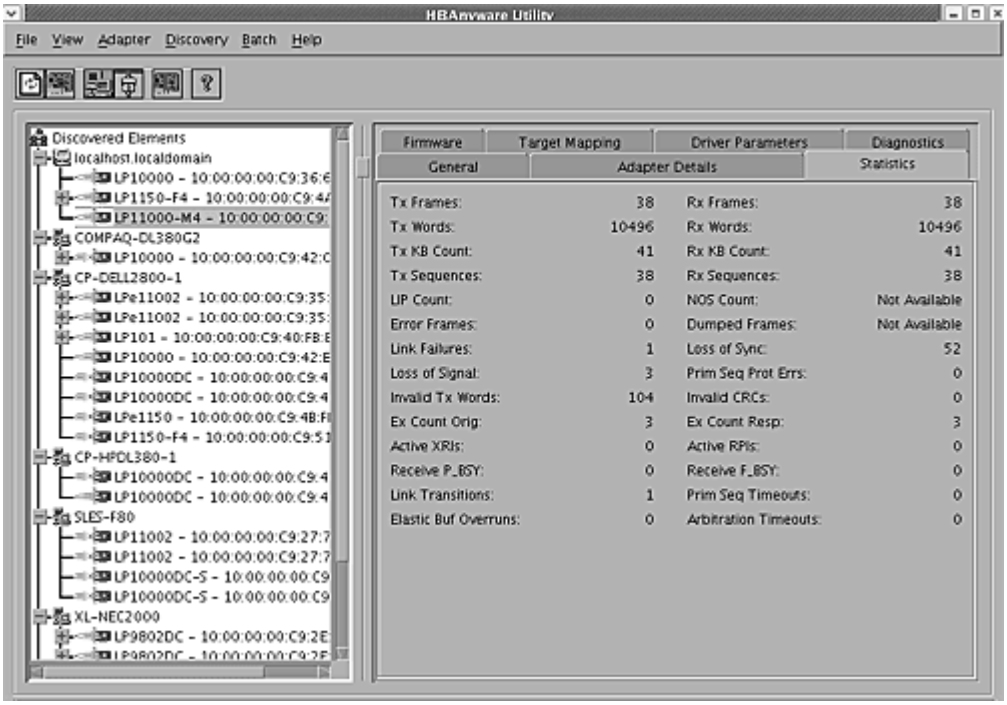


Figure 15: HBAnyware Utility, Statistics Tab

Port Statistics Field Definitions

- Tx Frames - Fibre Channel frames transmitted by this HBA port.
- Tx Words - Fibre Channel words transmitted by this HBA port.
- Tx KB Count - Fibre Channel kilobytes transmitted by this HBA port.
- Tx Sequences - Fibre Channel sequences transmitted by this HBA port.
- LIP count - The number of loop initialization primitive (LIP) events that have occurred for the port. This field is not supported if the topology is not arbitrated loop. Loop initialization consists of the following:
    - Temporarily suspend loop operations.
    - Determine whether loop capable ports are connected to the loop.
    - Assign AL_PA IDs.
    - Provide notification of configuration changes and loop failures.
    - Place loop ports in the "monitoring" state.
- Error Frames - The number of frames received with cyclic redundancy check (CRC) errors.
- Link Failures - The number of times the link failed. A link failure is a possible cause of a timeout.
- Loss of Signal - The number of times the signal was lost.
- Invalid Tx Words - The total number of invalid words transmitted by this HBA port.

- Ex Count Orig - The number of Fibre Channel exchanges originating on this port.
- Active XRIs - The number of active exchange resource indicators.
- Received P_BSY - The number of FC port-busy link response frames received.
- Link Transitions - The number of times the SLI port sent a link attention condition.
- Elastic Buf Overruns - The number of times the link interface has had its elastic buffer overrun.
- Rx Frames - The number of Fibre Channel frames received by this HBA port.
- Rx Words - The number of Fibre Channel words received by this HBA port.
- Rx KB Count - The received kilobyte count by this HBA port.
- Rx Sequences - The number of Fibre Channel sequences received by this HBA port.
- NOS count - This statistic is currently not supported for the SCSIport Miniport and Storport Miniport drivers, nor is it supported for arbitrated loop.
- Dumped Frames - This statistic is not currently supported for the SCSIport Miniport driver, the Storport Miniport driver or the driver for Solaris.
- Loss of Sync - The number of times loss of synchronization has occurred.
- Prim Seq Prot Errs - The primitive sequence protocol error count. This counter is incremented whenever there is any type of protocol error.
- Invalid CRCs - The number of frames received that contain CRC failures.
- Ex Count Resp - The number of Fibre Channel exchange responses made by this port.
- Active RPIs - The number of remote port indicators.
- Receive F_BSY - The number of Fibre Channel port-busy link response frames received.
- Primitive Seq Timeouts - The number of times a primitive sequence event timed out.
- Arbitration Timeouts - The number of times the arbitration loop has timed out. Large counts could indicate a malfunction somewhere in the loop or heavy usage of the loop.

Viewing Firmware Information

Use the Firmware tab to view current firmware versions, enable system BIOS and update firmware on remote and local HBAs. The update procedure is on page 53.

To view the firmware information:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Select an HBA in the discovery-tree.

4. Select the Firmware tab

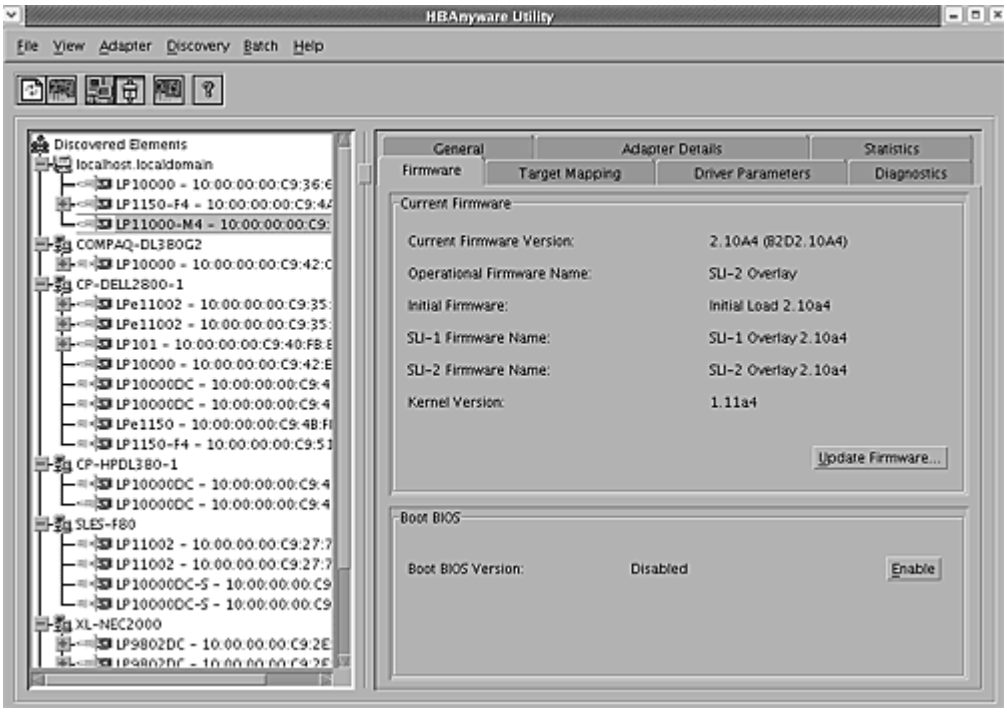


Figure 16: HBAnyware Utility, Firmware Tab

Firmware Field Definitions

Firmware Area

- Firmware Version - The Emulex firmware version number for this model of HBA.
- Operational Firmware Name - If visible, the name of the firmware that is operational.
- Initial Firmware - The firmware version stub responsible for installing the SLI code into its proper slot.
- SLI-1 Firmware Name - The name of the SLI-1 firmware overlay.
- SLI-2 Firmware Name - The name of the SLI-2 firmware overlay.
- Kernel Version - The version of the firmware responsible for starting the driver.

Firmware Tab Buttons

- **Enable/Disable** - Click to enable or disable the boot code.
- **Update Firmware** - Click to this button to display the HBAnyware Firmware Download dialog box. Using the HBAnyware Firmware Download dialog box, browse to the file you wish to download and download the file. See the “Update Firmware Using HBAnyware” topic on page 53 for more information.

Viewing Target Mapping

Use this tab to view target mapping. The Target Mapping tab is read-only. See “Using udev for Persistent Naming” on page 72 to learn how to create persistent naming.

To view target mapping:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Select an HBA in the discovery-tree.
4. Select the Target Mapping tab.

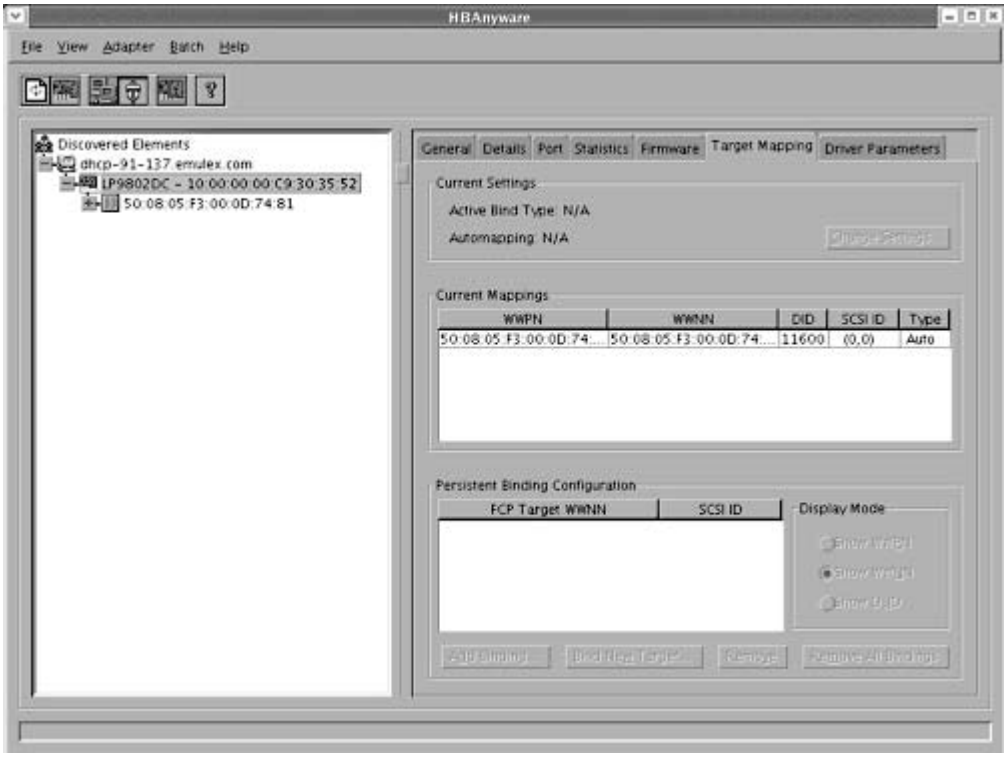


Figure 17: HBAnyware Utility, Target Mapping Tab

Target Mapping Field Definitions

Current Settings Area

- Active Bind Type -N/A
- Automapping - N/A

Current Mappings Table

- This table lists current mapping information for the selected HBA.

Persistent Binding Configuration Table

- N/A

Display Mode Radio Buttons

- N/A

Target Mapping Buttons

- N/A

Viewing HBA Information Using the lputil Utility

The LightPulse Diagnostic utility (lputil) allows you to view information for a selected HBA.

To view HBA information using the lputil utility:

1. Start the lputil utility. The Main menu is displayed:

Figure 18: lputil Main Menu

2. Enter 2, Adapter Information.

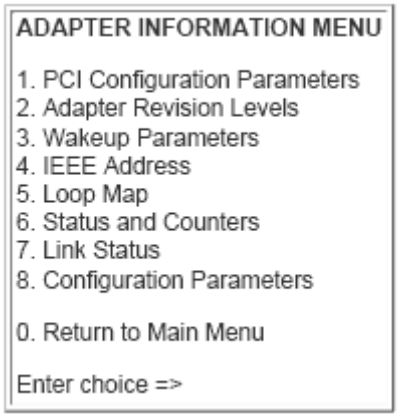


Figure 19: lputil Adapter Menu

If you have multiple HBAs, a list is displayed, you select an HBA and the Adapter Information Menu opens. If you have only one HBA, the Adapter Information Menu opens for that HBA.

The Adapter Information Menu displays the following information:

- PCI Configuration Parameters - Parameters from the PCI configuration space on the HBA. Information includes vendor ID, device ID, base addresses, ROM address, header type, subclass and base class.
- Adapter Revision Levels - Firmware revision levels, including kernel and overlay version information.
- Wakeup Parameters - BIOS status and version, as well as SLI (service level interface).
- IEEE Address - The HBA board address.
- Loop Map - If you are using arbitrated loop topology, this option shows information about your connected devices, such as AL_PA and D_ID.
- Status and Counters - Byte, frame, sequence and busy counts.

- Link Status - Tracks activities such as link failure, loss of sync, and elastic overlay.
- Configuration Parameters - D_ID topology, and timeout values for link failures and loss of sync.

Resetting HBAs

You can reset HBAs using either the HBAnyware or lputil utilities.

- The HBAnyware utility allows you to reset remote and local HBAs.
- The lputil utility allows you to reset local HBAs only.

Caution: Do not reset your HBA while copying or writing files. This could result in data loss or corruption.

Resetting the HBA Using the HBAnyware Utility

To reset the HBA using the HBAnyware utility:

1. Start the HBAnyware utility.
2. In the discovery-tree, select the HBA you want to reset.
3. Do one of the following:
   - From the menu bar, click **Adapter**, and then click **Reset HBA**.
   - Click the **Reset HBA** button.
4. The following warning screen appears:

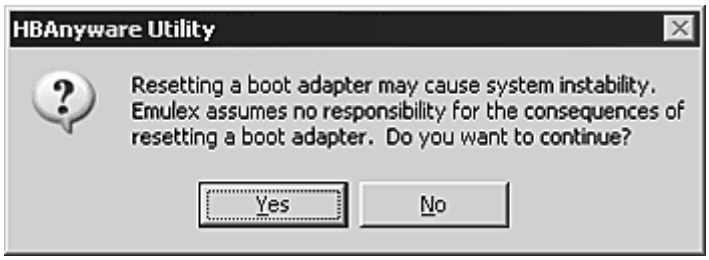

HBAnyware Utility
Resetting a boot adapter may cause system instability. Emulex assumes no responsibility for the consequences of resetting a boot adapter. Do you want to continue?
Yes
No

Figure 20: HBAnyware Utility, Reset Warning Screen

5. Click **Yes**. The HBA resets.

The reset may require several seconds to complete. While the HBA is resetting, the status bar shows “Reset in progress.” When the reset is finished, the status bar shows “Ready”.

Resetting the HBA Using the lputil Utility

The LightPulse Diagnostic utility (lputil) allows you to reset a local HBA.

To reset the HBA using the lputil utility:

1. Start the lputil utility. The Main menu is displayed.
2. Enter 4, Reset Adapter.
3. If you have multiple HBAs, select the HBA you want to reset.

Resetting the HBA runs self tests and reestablishes links (causes discovery of devices). Once the HBA has been successfully reset, the Main menu is displayed.

Updating Firmware

You can update firmware using either the HBAnyware or lputil utilities.

- The HBAnyware utility allows you to update firmware on remote and local HBAs.
- The lputil utility allows you to update firmware on local HBAs only.

Updating Firmware Using the HBAnyware Utility

Prerequisites

- The Emulex driver for Linux (including lpfcdfc) is installed properly.
- The HBAnyware utility is installed properly.
- The firmware file has been downloaded from the Emulex Web site and extracted.

Note: For OEM branded HBAs, see the OEM's Web site or contact the OEM's customer service department or technical support department for the firmware files.

Procedure

To update firmware using the HBAnyware utility:

1. Start the HBAnyware utility.
2. In the discovery-tree, select the HBA onto which you want to update firmware.
3. Select the Firmware tab.

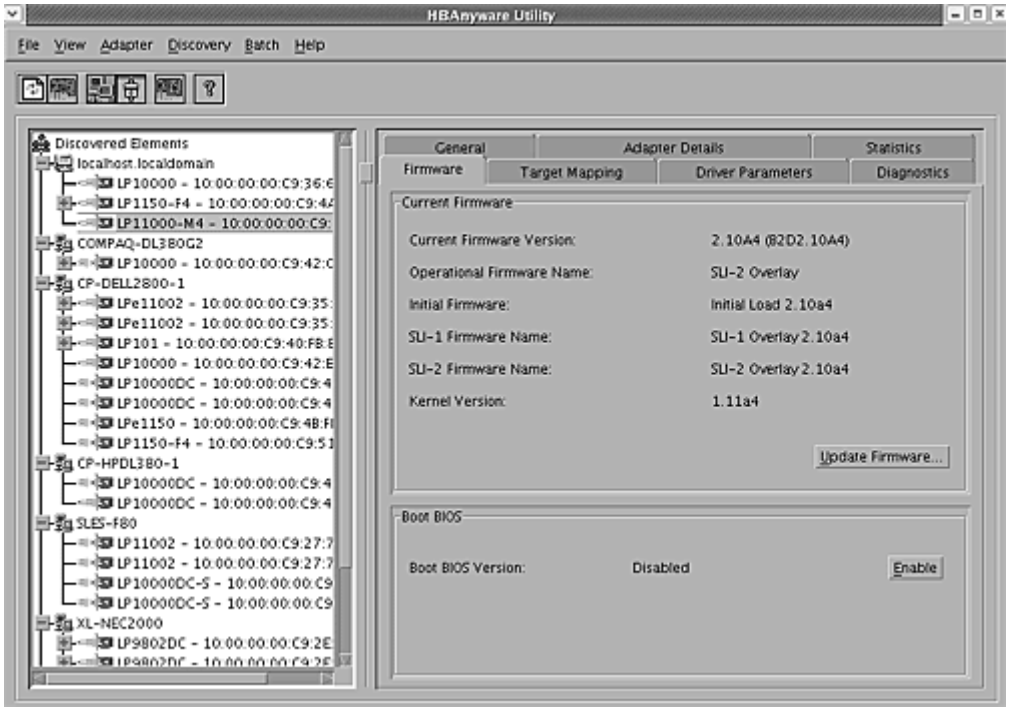


Figure 21: HBAnyware Utility, Firmware Tab

4. Click **Update Firmware**. The Firmware Download dialog box appears.

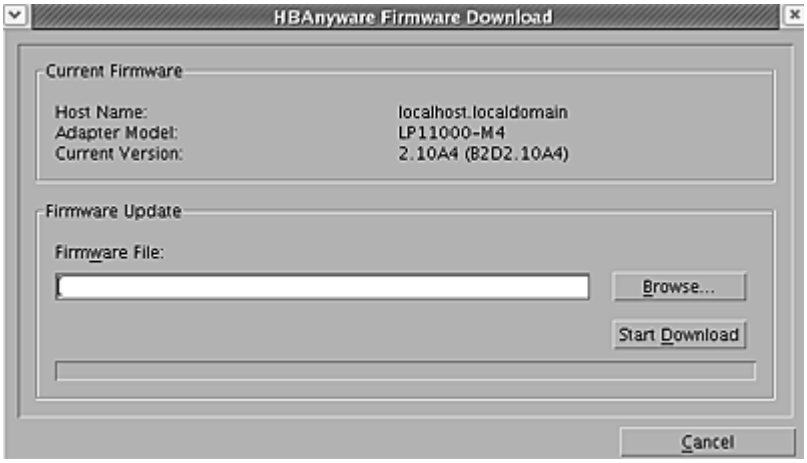


Figure 22: HBAnyware Utility, Firmware Download Dialog Box

5. Click **Browse**. The Firmware File Selection dialog box appears.

Figure 23: HBAnyware Utility, Firmware File Selection Dialog Box

6. Navigate to the extracted firmware file you wish to download. Select the file and click **OK**. A status bar shows the progress of the download and indicates when the download is complete.
7. Click **Start Download**.

If you are updating the firmware on a dual-channel HBA, repeat steps 2 through 7 to update the firmware on the second port or use the “Updating Firmware (Batch Mode) Using the HBAnyware Utility” procedure on page 55.

Note: If the state of the boot code on the board has changed, this change will be reflected immediately on the General tab.

Updating Firmware (Batch Mode) Using the HBAnyware Utility

Loading firmware in batch mode differs from its non-batch counterpart in that it enables you to install firmware on multiple HBAs in a single step. Batch firmware loading is restricted to a single firmware file and to all accessible HBAs for which that file is compatible.

Note: Stop other HBAnyware utility functions while batch loading is in progress.

Prerequisites

- The firmware file has been downloaded from the Emulex Web site and extracted to the Emulex Repository folder (RMRepository). This folder is in /usr/sbin/HBAnyware/RMRepository.

Procedure

To batch load firmware using the HBAnyware utility:

1. Start the HBAnyware utility.
2. From the menu bar, select **Batch** and click **Download Firmware.**

Note: You do not need to select a particular tree element for this operation.

3. When the Batch Firmware File dialog box appears, browse to locate and select the firmware file to download. Click **Open**.

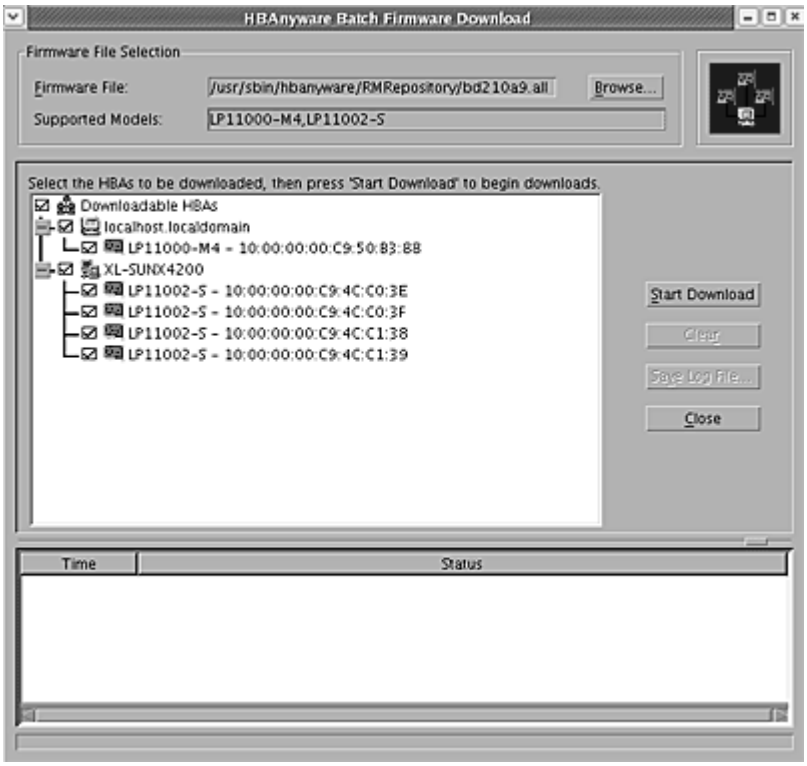


Figure 24: HBAnyware Utility, Batch Firmware Download Dialog Box

4. A tree-view appears showing all HBAs and their corresponding hosts for which the selected firmware file is compatible.

5. Check boxes next to the host and HBA entries are used to select or deselect an entry. Checking an HBA selects or removes that HBA; checking a host removes or selects all eligible HBAs for that host.
6. When selection/deselection is complete, click **Start Download**.
7. Once downloading begins, the tree-view displays the progress. As firmware for a selected HBA is being downloaded, it appears orange in the tree-view. Once successful downloading is complete, the entry changes to green. If the download failed, the entry is changed to red.

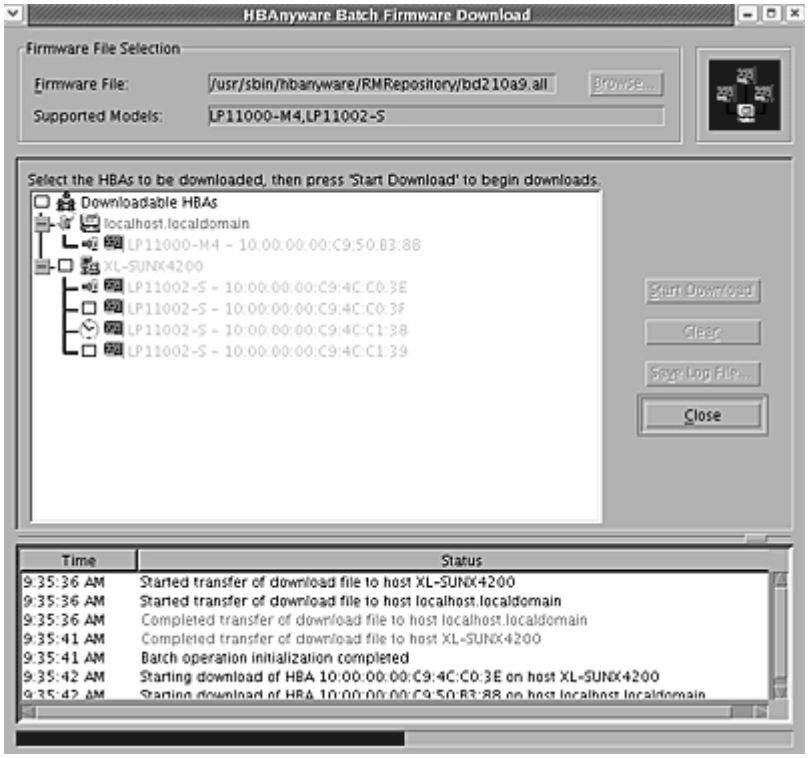

HBAnyware Batch Firmware Download
Firmware File Selection
Firmware File:
/usr/sbin/hbanyware/RMRepository/bd210a9.all
Browse...
Supported Models:
LP11000-M4,LP11002-S
Select the HBAs to be downloaded, then press 'Start Download' to begin downloads.
Downloadable HBAs
localhost.localdomain
LP11000-M4 - 10:00:00:00:C9:50:B3:88
XL-SUNX4200
LP11002-S - 10:00:00:00:C9:4C:C0:3E
LP11002-S - 10:00:00:00:C9:4C:C0:3F
LP11002-S - 10:00:00:00:C9:4C:C1:38
LP11002-S - 10:00:00:00:C9:4C:C1:39
Start Download
Clear
Save Log File...
Close
Time
Status
9:35:36 AM Started transfer of download file to host XL-SUNX4200
9:35:36 AM Started transfer of download file to host localhost.localdomain
9:35:36 AM Completed transfer of download file to host localhost.localdomain
9:35:41 AM Completed transfer of download file to host XL-SUNX4200
9:35:41 AM Batch operation initialization completed
9:35:42 AM Starting download of HBA 10:00:00:00:C9:4C:C0:3E on host XL-SUNX4200

Figure 25: HBAnyware Utility, Firmware Download Dialog Box with Completed Download

8. When downloading is complete, you can click **Print Log** to get a hard copy of the activity log.
9. Click **Close** to exit the batch procedure.

Updating Firmware Using the lputil Utility

The lputil utility enables you to update firmware on a local HBA.

Prerequisites

- The driver for Linux (including the Application Helper Module) is installed properly.
- The lputil utility is installed properly.
- The firmware file has been downloaded to a local drive.

Caution: If you are using the lputil utility to update firmware on an LP1005DC, you must use lputil version 2.0a3 or later.

Procedure

Caution: Do not interrupt this process or power down the system until the process is complete.

To update firmware using the lputil utility:

1. Start the lputil utility. The Main menu is displayed.
2. Enter 3, Firmware Maintenance.
3. If prompted, choose the HBA that is being updated.
4. Enter 1, Load Firmware Image.
5. Enter the full path to the firmware file.

   If you are updating the firmware on a dual-channel HBA, repeat steps 3 through 5 to update the firmware on the second port.
6. Enter 0 twice to exit the utility.

The new firmware is transferred to flash ROM.

Enabling or Disabling an HBA's BIOS

Enabling the BIOS is a two-step process:

1. Enable the HBA BIOS (x86 BootBIOS, FCode or EFIBoot) to read the Emulex boot code on the HBA (using the HBAnyware or lputil utilities).
2. Enable the HBA to boot from SAN (using the BIOS utility).

Enabling or Disabling an HBA's BIOS Using the HBAnyware Utility

Prerequisites

- The Emulex driver for Linux is installed properly.

Procedure

To enable or disable the HBA BIOS using the HBAnyware utility:

1. Start the HBAnyware utility.
2. In the discovery-tree, select the HBA whose BIOS you wish to enable or disable.

3. Select the Firmware Tab.

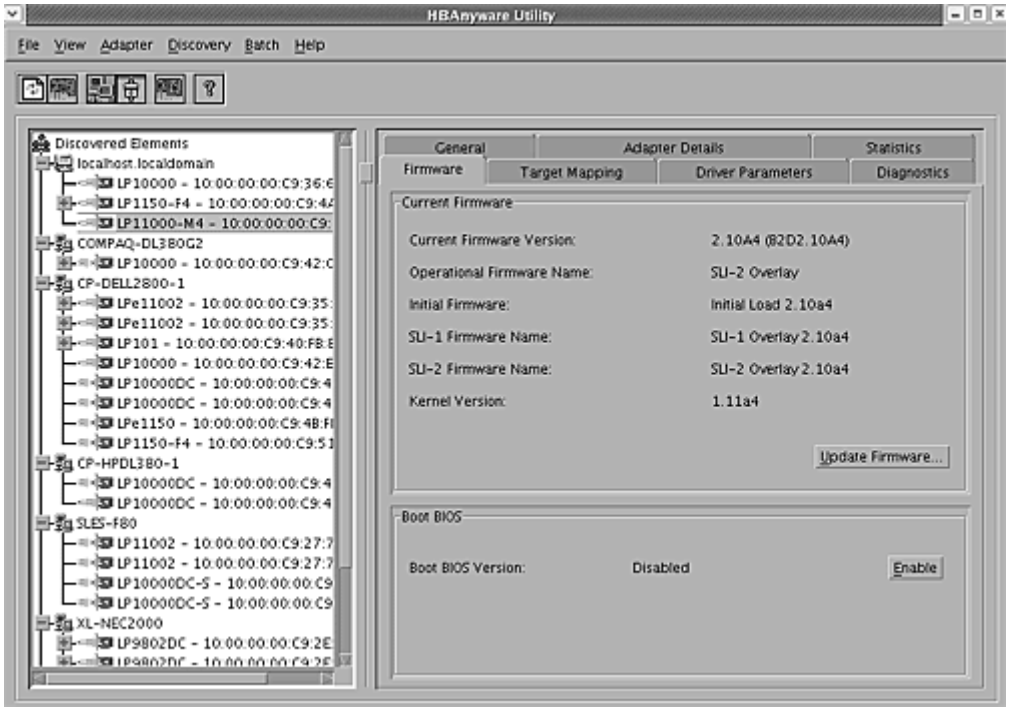


Figure 26: HBAnyware Utility, Firmware Tab with BIOS Disabled

4. To enable the BIOS, click **Enable**. The button title changes from **Enable** to **Disable**.

   Or

   To disable the BIOS, click **Disable**. The button title changes from **Disable** to **Enable**.

   Note: If the BIOS state on the board changes, the change reflects immediately on the General tab

   If you are updating x86 BootBIOS, you must also enable the HBA to boot from SAN using the BIOS utility; see the documentation that accompanies the boot code for more information.

Enabling or Disabling an HBA's BIOS Using the lputil Utility

Prerequisites

- The Emulex driver for Linux is installed properly.
- The lputil utility is installed properly.
- The x86 BootBIOS file is properly installed.

Procedure

To enable or disable the HBA BIOS using the lputil utility:

1. Start the lputil utility. The Main menu is displayed.
2. Enter 3, Firmware Maintenance.
3. If prompted, choose the HBA that is being updated.
4. From the Firmware Maintenance menu, enter 6, Boot BIOS Maintenance.
    - If the BIOS is currently disabled, press 1, Enable Boot BIOS, to enable the BIOS.
    - If the BIOS is already enabled, press 1, Disable Boot BIOS, to disable the BIOS.
    - If the BIOS is not currently loaded, the following message is displayed:
      `There is no Boot BIOS found on adapter`
5. Enter 0 twice to exit.
6. If you are updating x86 BootBIOS, you must also enable the HBA to boot from SAN using the BIOS utility; see the documentation that accompanies the boot code for more information.

Configuring the Driver

You can configure the driver using the following methods:

Note: Driver parameter changes made using the HBAnyware utility or modprobe.conf persist if the driver is uninstalled. To return to the default settings, you must modify the settings in modprobe.conf.

- Setting driver parameters using the HBAnyware utility.
- Setting module parameters in /etc/modprobe.conf.
- Specifying parameters when loading the driver manually.
- Through the sysfs interface (for parameters which can be changed after loading the driver).

Setting Driver Parameters Using the HBAnyware Utility

The Driver Parameters tab and Host Driver Parameter tab enable you to modify driver parameters for a specific HBA or all HBAs in a host.

For example, if you select a host in the discovery-tree, you can globally change the parameters for all HBAs in that host. If you select an HBA in the discovery-tree, you can change the lpfc_use_adisc, lpfc_log_verbose and the lpfc_nodev_tmo parameters for only that HBA.

For each parameter, the Driver Parameters tab and Host Driver Parameters tab shows the current value, the range of acceptable values, the default value, and whether the parameter is dynamic (a dynamic parameter allows the change to take effect without restarting the HBA or rebooting the system). You can make parameter changes persistent after a reboot of the system. You can also restore parameters to their default settings.

You can also apply driver parameters for one HBA to other HBAs in the system using the Driver Parameters tab. When you define parameters for an HBA, you create a .dpv file. The .dpv file contains the parameters for that HBA. After you create the .dpv file, the HBAnyware utility enables you to apply the .dpv file parameters to multiple HBAs in the system, thereby simplifying multiple HBA configuration. See “Creating the Batch Mode Driver Parameters File” on page 63 for more information.

Note: The Linux 2.6 kernel only supports setting the log_verbose, nodev_tmo and use_adisk driver parameters for individual HBAs. You must apply other driver parameters to all HBAs contained in the host.

Setting Driver Parameters for an HBA

To change the driver parameters for an HBA:

1. Start the HBAnyware utility.
2. Do one of the following:
   - From the menu bar, click **View**, then click **Sort by Host Name**.
   - From the toolbar, click the **Sort by Host Name** button.
3. In the discovery-tree, select the HBA whose parameters you wish to change.

4. Select the Driver Parameters tab (Figure 27). The parameter values for the selected HBA are displayed.

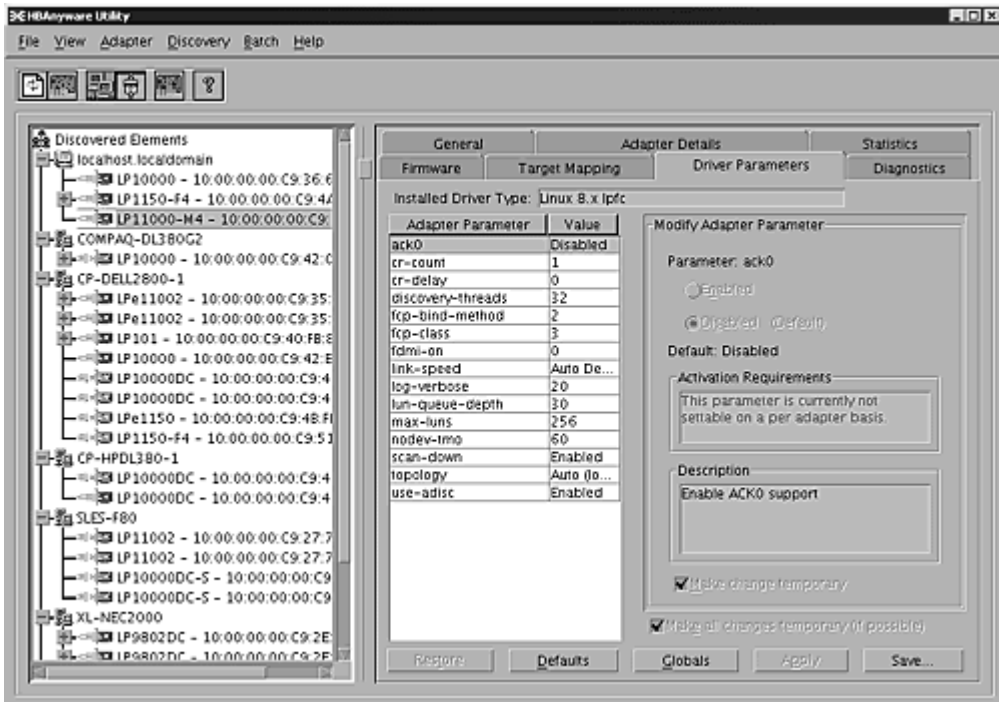


Figure 27: HBAnyware Utility, HBA Selected - Driver Parameters Tab

5. In the Driver Parameters tab, click the parameter that you want to change. A description of the parameter appears on the right side of the dialog box.
6. Enter a new value in the Value field in the same hexadecimal or decimal format as the current value. If the current value is in hexadecimal format, it is prefaced by "0x" (for example, 0x2d). You may enter a new hexadecimal value without the "0x". For example, if you enter ff10, this value is intepreted and displayed as "0xff10".
7. If you want the change to be temporary (causing the parameter to revert to its last permanent setting when the system is rebooted), check the "Make change temporary" box. This option is available only for dynamic parameters.
8. If you are making changes to multiple parameters, and you want all the changes to be temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
9. Click **Apply**.

Restoring All Parameters to Their Earlier Values

If you changed parameters, but did not click **Apply** and you want to restore the parameters to their last saved values, click **Restore**.

Resetting All Default Values

If you want to reset all parameter values to their default (factory) values, click **Defaults**.

Setting Driver Parameters for a Host

To change the driver parameters for HBAs installed in a host:

1. Start the HBAnyware utility.
2. Do one of the following:
   - From the menu bar, click **View**, then click **Sort by Host Name**.
   - From the toolbar, click the **Sort by Host Name** button.
3. In the discovery-tree, click the host whose HBA driver parameters you wish to change.
4. Click the Host Driver Parameters tab. If there are HBAs with different driver types installed, the installed Driver Types menu shows a list of all driver types and driver versions that are installed on the HBAs in the host. Select the driver whose parameters you wish to change. This menu does not appear if all the HBAs are using the same driver.
5. In the Host Driver Parameters tab, click the parameter that you want to change. A description of the parameter appears on the right side of the dialog box.

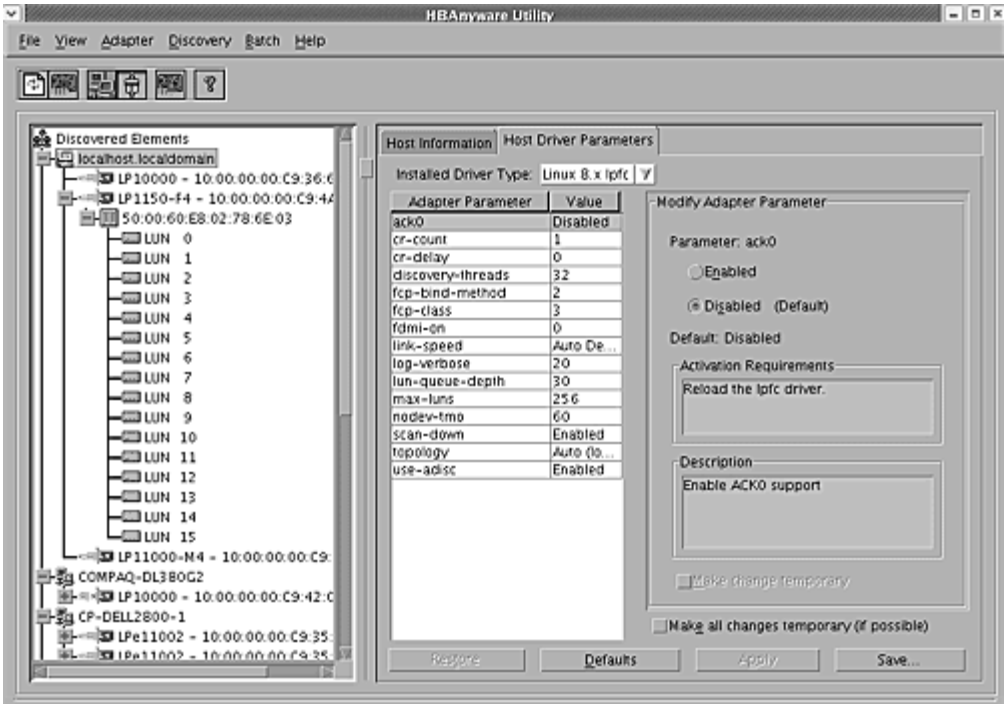


Figure 28: HBAnyware Utility, Host Selected - Driver Parameters Tab

6. Enter a new value in the Value field. You must enter values in decimal or hexadecimal format, depending on how the current value is presented. If the value is in hexadecimal format, it is prefaced by "0x" (for example 0x2d).
7. If you want the change to be temporary (causing the parameter to revert to its last permanent setting when the system is rebooted), check the "Make change temporary" box. This option is available only for dynamic parameters.
8. If you are making changes to multiple parameters, and you want all the changes to be temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
9. Click **Apply**.

Restoring All Parameters to Their Earlier Values

If you changed parameters, but did not click **Apply** and you want to restore the parameters to their last saved values, click **Restore**.

Resetting All Default Values

If you want to reset all parameter values to their default (factory) values, click **Defaults**.

Changing Non-dynamic Parameter Values

To change non-dynamic parameter values:

1. Navigate to the /usr/sbin/hbanyware directory and run the scripts to stop the HBAnyware utility processes. Type:

   ```
   ./stop_hbanyware
   ```
2. Stop all I/O to lpfc attached devices.
3. Unload the lpfcdfc driver. Type:

   ```
   rmmod lpfcdfc
   ```
4. Unload the lpfc driver. Type:

   ```
   rmmod lpfc
   ```
5. Reload the driver.Type:

   ```
   modprobe lpfc
   modprobe lpfcdfc
   ```

   The HBAnyware services will start automatically when you launch the application.

   For these changes to persist after a reboot you must create a new ramdisk image. See “Creating a New Ramdisk Image” on page 67 to learn how.

Creating the Batch Mode Driver Parameters File

You can apply driver parameters for one HBA to other HBAs in the system using the Driver Parameters tab. When you define parameters for an HBA, you create a .dpv file. The .dpv file contains the parameters for that HBA. After you create the .dpv file, the HBAnyware utility enables you to apply the .dpv file parameters to multiple HBAs in the system, thereby simplifying multiple HBA configuration.

To create the .dpv file:

1. Start the HBAnyware utility.
2. Select the HBA whose parameters you want to apply to other HBAs from the discovery-tree.
3. Select the Driver Parameters tab. Set driver parameters (see Figure 27 on page 61).

4. After you define the parameters for the selected HBA, click **Save Settings**. The Select Driver Parameter File dialog box appears. Use the dialog box to select where to save the file or to rename the file. Click **Save**. The Save Driver Parameters dialog box appears.

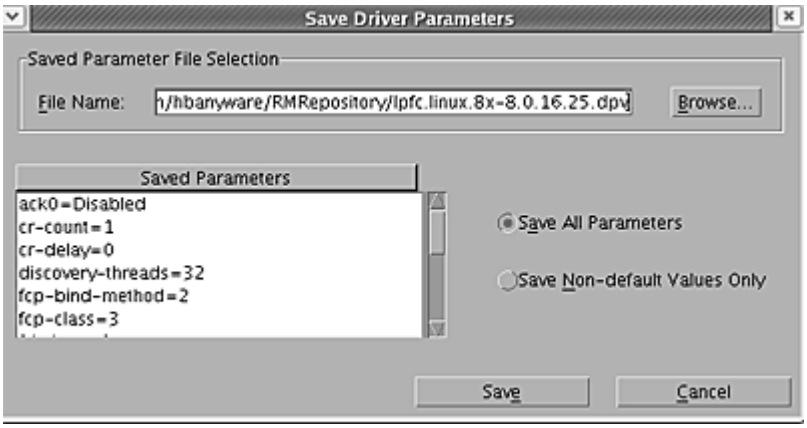


Figure 29: HBAnyware Utility, Save Driver Parameters Dialog Box

5. The two radio buttons allow you to choose the type of parameters to save. You can save all parameters or only those parameters whose current values differ from their corresponding default values.
6. A list of the saved parameters and their current values show in the Saved Parameters box.
7. Click **Save**.

Assigning Batch Mode Parameters to HBAs

After you create the batch mode parameters (.dpv) file, you can assign its parameters to multiple HBAs. Assigning batch mode parameters make it easy to configure multiple HBAs. See “Creating the Batch Mode Driver Parameters File” on page 63 to learn how to create the .dpv file.

To assign batch mode parameters to HBAs:

1. Start the HBAnyware utility.
2. From the HBAnyware utility menu, click **Batch** and select **Update Driver Parameters**. (You do not need to select any discovery-tree elements at this time.) The Select Driver Parameter File dialog box appears.

3. Select the file whose parameters you wish to apply and click **Open**. The Batch Driver Parameter Update dialog box shows all the batch file compatible HBAs with a check mark beside them.

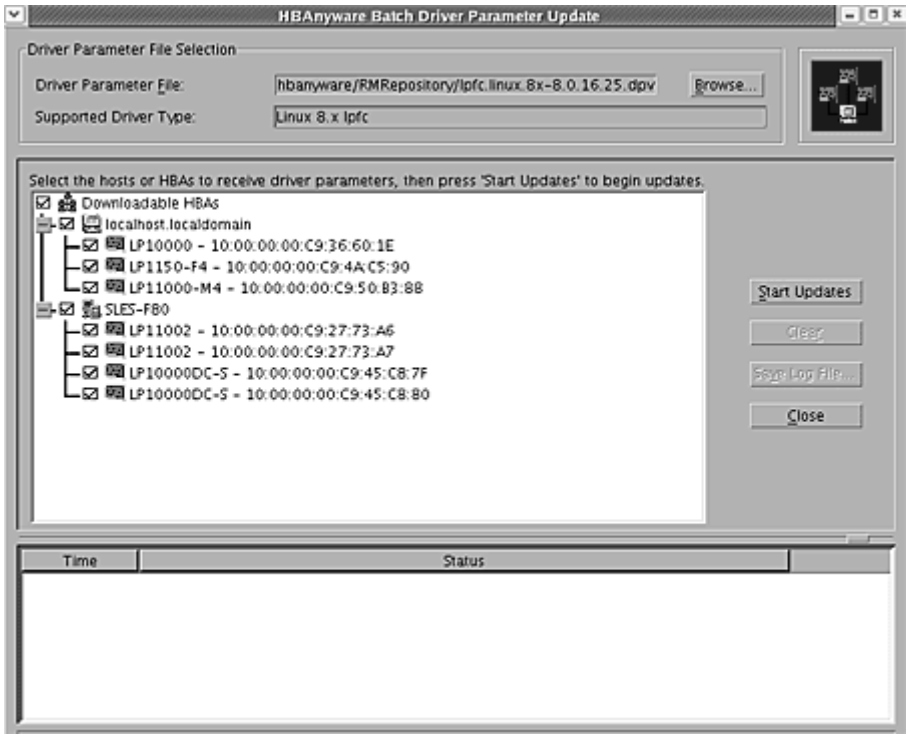


Figure 30: HBAnyware Utility, Batch Driver Parameters Update Dialog Box

4. Click **Start Updates**. The HBAnyware utility Batch Driver Update dialog box shows the current status of the update. When the update completes, a final summary shows the number of HBAs that were successfully processed, and the number of HBAs for which one or more parameter updates failed.

   If you wish, click **Print Log** to print a report of the update.

Driver Configuration Methods Using modprobe and /etc/modprobe.conf

The following sections describe how to set driver parameters using the modprobe command and by manually editing /etc/modprobe.conf.

Note: Emulex recommends using the HBAnyware utility or the hbacmd to change parameters.

Temporary Configuration Method

When you manually load the driver as a module using the modprobe command and change one or more driver parameter values, it is a temporary configuration. These changes are considered temporary because they are valid for the current session only or until the driver is manually loaded again. Using the insmod command requires no editing or saving. This temporary configuration method overrides the modprobe.conf file for the current session.

Values can be expressed in hexadecimal or decimal notation.

Example of Temporary Configuration

You want to temporarily set lun_queue_depth to 20 (default is 30) for all host bus adapters in your system. Load the driver with the following command:

```
modprobe lpfc lpfc_lun_queue_depth=20
```

Note: You cannot override parameters set in modprobe.conf

Persistent Configuration Method

To make the driver parameters persistent across module loads and reboots, modify the /etc/modprobe.conf file. If driver parameters are modified in /etc/modprobe.conf, the driver must be reloaded for the parameters to take effect. Also a new ramdisk image will be needed. See “Creating a New Ramdisk Image” on page 67 to learn how.

The driver parameters are specified in /etc/modprobe.conf via the "options" command. For example the following sets the verbose flag.

```
options lpfc lpfc_log_verbose=0xffff
```

If the same option is specified in both the /etc/modprobe.conf and on the modprobe command line, the option setting in the command line takes precedence.

Temporary Driver Configuration by Read/Write to sysfs

Sysfs is a virtual filesystem that exposes the structure of the system to the user. It also includes interfaces to driver parameters through which the driver parameters can be viewed and modified. Since these interfaces are available only after driver load, only those parameters that can be modified dynamically can be changed in this manner. Nevertheless all driver parameters can be read through sysfs. It is important to note that sysfs changes exist only for the lifetime of the driver load and are lost on driver unload or reboot.

The sysfs filesystem is mounted and available as /sys. We must first identify the scsi_host which represents the HBA for which we wish to modify the driver parameters. All scsi_hosts bound to the lpfc driver can be viewed with the following command:

```
# ls -d /sys/bus/pci/drivers/lpfc/*/host*
```

Assuming we are interested in HBA scsi_host 7, we can list the driver parameters for this particular HBA as:

```
#ls -l /sys/class/scsi_host/host7/lpfc*
```

An example output is as follows:

```
-r--r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_ack0
-rw-r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_fcp_bind_method
-r--r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_fcp_class
-rw-r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_fdmi_on
-r--r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_link_speed
-rw-r--r--  1 root root 4096 Feb 28 15:34 /sys/class/scsi_host/host7/lpfc_log_verbose
-r--r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_lun_queue_depth
-rw-r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_max_luns
-rw-r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_nodev_tmo
-rw-r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_scan_down
-r--r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_topology
-rw-r--r--  1 root root 4096 Feb 28 17:03 /sys/class/scsi_host/host7/lpfc_use_adisc
```

Notice that the driver parameters are available as files. Reading a file displays the current value of a driver parameter. If the permissions allow it, you can write a value to the file and it will take effect immediately.

For example:

```
[root@emulex]# cat /sys/class/scsi_host/host7/lpfc_log_verbose
0
```

Notice that the current value of lpfc_log_verbose is zero. To set it to 0xffff:

```
[root@emulex]# echo 0xffff > /sys/class/scsi_host/host7/
lpfc_log_verbose
[root@emulex]# cat /sys/class/scsi_host/host7/lpfc_log_verbose
0xffff
```

Creating a New Ramdisk Image

The lpfc-install script creates a ramdisk containing the lpfc driver for the currently running kernel.

Note: You must perform this step whenever the lpfc options in /etc/modprobe.conf are changed and you want the change to take affect on the next reboot.

For Installed lpfc Driver Kits

To create a new initial ramdisk image:

1. su to ‘root’.
2. Type:

   ```
   cd /usr/src/lpfc
   ```

3. Execute the lpfc-install script using the '--createramdisk' option. Type:

```
./lpfc-install --createramdisk
```

For Distribution In-Box lpfc Drivers

To create a new initial ramdisk image:

- For SLES10 PPC64 architecture distributions type:

```
# mkinitrd -k vmlinux -i initrd
```

- For SLES10 non-PPC64 architecture distributions type:

```
# mkinitrd -k vmlinuz -i initrd
```

Dynamically Adding LUNs and Targets

The Emulex driver for Linux enables you to dynamically add LUNs and targets without unloading or reloading the lpfc module and without resetting the adapter.

To rescan an HBA's targets with sysfs given the HBA's host number (in this example 3), type:

```
echo "- - -" > /sys/class/scsi_host/host3/scan
```

To limit the rescan to a particular target, given the HBA's host number (in this example 3) and the target number (in this example 2), type:

```
echo "- 2 -" > /sys/class/scsi_host/host3/scan
```

You can also use the Emulex lun_scan script in /usr/sbin/lpfc.

Downloading PCI Configuration

Note: Select this option only if you are familiar with PCI configuration registers.

To download the PCI configuration data:

1. Start the lputil utility.
2. From the lputil Main menu, select 3, Firmware Maintenance.The Firmware Maintenance menu is displayed.
3. If you have more than one adapter in your system, select the adapter for which you want to download a PCI configuration.
4. Select 5, Load PCI Configuration File. PCI configuration data is contained in .cfl files, which can be used across any supported platform.
5. Enter the region in flash ROM to download the data, and press <Enter>. You can download one of three data sets for the PCI configuration registers.
    - Default PCI configuration region
    - PCI configuration region 1
    - PCI configuration region 2
6. Upon completion, press 0 to return to Main menu.
7. Press 0 to exit the utility.
8. Power down the system.
9. Restart the system to load new configuration data.

Driver Parameters Reference Table

The driver parameters determine some aspects of the driver behavior. The following tables list the driver parameters. Some driver parameters can be modified and take effect only on a driver load while others can be modified dynamically and take effect immediately. The tables also list the default, minimum and maximum values for these parameters.

Table 3: lpfc Static Parameters (Requires a driver reload to change)

Variable	Default	Min	Max	Comments	Visible using sysfs
lpfc_ack0	0	0=Off	1=On	Uses ACK0 for class 2.	Yes
lpfc_cr_count	1	1	255	This parameter determines the values for I/O coalescing for cr_delay (msec) or cr_count outstanding commands.	No
lpfc_cr_delay	0	0	63	This parameter determines the values for I/O coalescing for cr_delay (msec) or cr_count outstanding commands.	No
lpfc_discovery_threads	32	1	64	Specifies the maximum number of ELS commands that can be outstanding for a discovery. Note: The discovery_threads parameter will default to a value of 64 for private loop topologies regardless of the configured value. If there are multiple ports configured on the host the value of 64 will only be used for those ports that are connected in a private loop topology. The configured value will be used for all other ports.	No
lpfc_fcp_class	3	2	3	The Fibre Channel class for FCP data transmission.	Yes
lpfc_link_speed	0	0=auto select 1=1G 2=2G 4=4G		Sets link speed.	Yes
lpfc_hba_queue_depth	8192	32	8192	The maximum number of FCP commands that can queue to an Emulex HBA.	Yes

Table 3: lpfc Static Parameters (Requires a driver reload to change) (Continued)

Variable	Default	Min	Max	Comments	Visible using sysfs
lpfc_lun_queue_depth	30	1	128	The default maximum commands sent to a single logical unit (disk).	Yes
lpfc_topology	0	0x0=loop then P2P 0x2=P2P only 0x4=loop only 0x6=P2P then loop		Fibre Channel link topology (defaults to loop, if it fails attempts point-to-point mode).	Yes
lpfc_fdmi_on	0	0	2	False (0) if disabled. (1) or (2) if enabled depending on type of support needed.	Yes
lpfc_scan_down	1	0=Off	1=On	Selects method for scanning ALPA to assign a SCSI ID.	Yes
lpfc_max_luns	256	1	32768	Specifies the maximum number of LUN IDs per target. A value of 20 means LUN IDs from 0 to 19 are valid. The SCSI layer will scan each target until it reaches the specified LUN ID.	Yes
lpfc_multi_ring_support	1	1	2	Determines the number of primary SLI rings over which to spread IOCB entries.	No
lpfc_poll	0	1= poll wiith interupts enabled 3 = poll and disable FCP ring interrupts		Sets FCP ring polling mode control.	Yes
lpfc_poll_tmo	10	1	255	Milliseconds the driver waits between polling FCP ring interrupts.	Yes

All lpfc dynamic parameters are read/write using sysfs.

Table 4: lpfc Dynamic Parameters (Do not require a driver reload to change)

Variable	Default	Min	Max	Comments
lpfc_log_verbose	0x0	0x0	0xffff	(bit mask) Extra activity logging.
lpfc_nodev_tmo	30	0	255	Seconds to hold I/O error if device disappears.

Table 4: lpfc Dynamic Parameters (Do not require a driver reload to change) (Continued)

Variable	Default	Min	Max	Comments
lpfc_use_adisc	0	0=Off	1=On	Sends ADISC instead of PLOGI for device discovery or RSCN.

Viewing Target Mapping

The Target Mapping tab enables you to view current target mapping.

Note: Persistent binding is not supported by the Linux 2.6 kernel or by the Emulex version 8 driver for Linux.

To view the Target Mapping tab:

1. Start the HBAnyware utility.
2. Do one of the following:
   - From the menu bar, click **View**, then click **Sort by Host Name**.
   - From the toolbar, click the **Sort by Host Name** button.
3. Select a target in the discovery-tree.

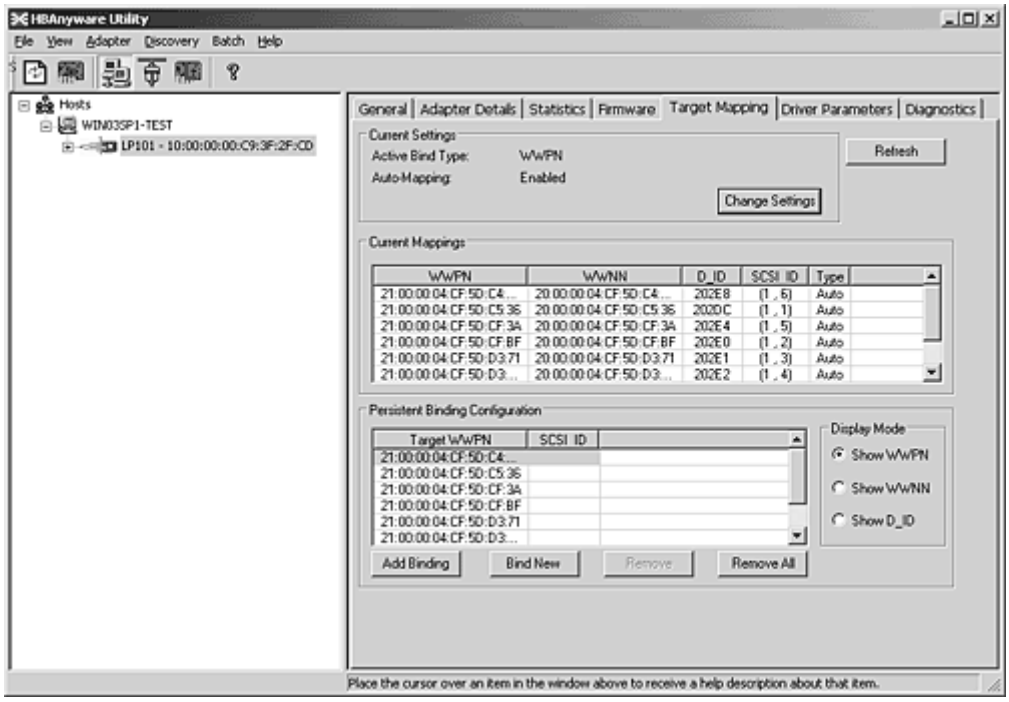


Figure 31: HBAnyware Utility, Target Mapping Tab

Using udev for Persistent Naming

SLES 10 is configured by default with udev to provide persistent names for hard disks, including FC attached disks.

Using udev to Discover Logical to Physical Mappings for sd Devices

Persistent names for sd devices are provided in the /dev/disk/by-id directory.

To find the persistent udev name for the disk which is currently sdc, type:

```
# cd /dev/disk/by-id
# ls -l | grep sdc
```

The sample output is shown below:

```
lrwxrwxrwx 1 root root  9 2006-08-01 19:08 scsi-32000000c5005d6e6 -> ../../sdc
```

In the above example, the disk has no partitions. If the disk had two partitions, the output would look like the following:

lrwxrwxrwx 1 root root 9 2006-08-01 19:08 scsi-32000000c5005d6e6 -> ../../sdc

lrwxrwxrwx 1 root root 10 2006-08-01 19:08 scsi-32000000c5005d6e6-part1 -> ../../sdc1

lrwxrwxrwx 1 root root 10 2006-08-01 19:08 scsi-32000000c5005d6e6-part2 -> ../../sdc2

Configuring the System to Boot From SAN Using Persistent Names

To use a persistent name for a boot device:

1. In /boot/grub/menu.lst, find the kernel line for the default boot. For example:

   kernel /boot/vmlinuz root=/dev/sda2 vga=0x314

2. Find the persistent name for the root partition (following "root=" on the kernel line) by using the instructions in "Using udev to Discover Logical to Physical Mappings for sd Devices" section on this page.
3. In the same file, /boot/grub/menu.lst, replace the text after "root=" with the partition's persistent name. For example:

   kernel /boot/vmlinuz root=/dev/disk/by-id/scsi-32000000c5005d6e6-part2 vga=0x314

4. Change any mounts listed in /etc/fstab which refer to this root partition by either it's /dev/sd name or a file system LABEL to use the persistent name as well.

Using udev with st Devices

The udev rules for tape devices are the same for disk devices. There must be a unique id that persists across initiator reboots and persists regardless of discovery order.

Another thing to consider is whether or not the tape device is one of many SCSI tape devices residing behind an FC controller, or if it is an FC-Tape device. If it an FC-Tape device, then the WWPN is unique and can be used to create the persistent name. In fact, the scsi_id program should return this as the unique identifier with a single digit prefix.

If the FC controller has multiple SCSI tape devices behind it, the WWPN is not unique and the persistent name must use multiple information elements to build the unique id.

Below are examples of each scenario. The first example is that of an FC-Tape device. This example uses scsi generic (sg) rather than the scsi tape driver.

```
[root@localhost ~]# scsi_id -g -s /class/scsi_generic/sg0
   350060b000029b592
```

The value return has a leading prefix of 3. This value is the NAA type and what follows is the controller's WWPN.

Below is an example of the same tape device and a scsi_id call. The response is the same.

```
[root@localhost ~]# scsi_id -g -s /class/scsi_tape/nst0
   350060b000029b592
```

In both examples, -g was needed because the vendor and model for this tape device were not in /etc/scsi_id.config.

Below is another example to a different FC-Tape Vendor. Notice that the answer is similar with respect to the leading digit and the WWPN.

```
[root@localhost ~]# /sbin/scsi_id -g -s /class/scsi_tape/nst0
35005076300015101
```

Below is an example of a FC-SCSI Tape device. Notice that when the Emulex driver loads, the scsi midlayer discovers the scsi tape devices as follows:

```
scsi scan: INQUIRY to host 14 channel 0 id 0 lun 0
scsi: unknown device type 12
  Vendor: ADIC      Model: SNC 4000         Rev: 42d4
  Type:   RAID                              ANSI SCSI revision: 03
Attached scsi generic sg5 at scsi14, channel 0, id 0, lun 0,  type 12
scsi scan: INQUIRY to host 14 channel 0 id 0 lun 1
  Vendor: ADIC      Model: Scalar 24        Rev: 227A
  Type:   Medium Changer                    ANSI SCSI revision: 02
Attached scsi generic sg6 at scsi14, channel 0, id 0, lun 1,  type 8
scsi scan: INQUIRY to host 14 channel 0 id 0 lun 2
  Vendor: IBM       Model: ULTRIUM-TD2      Rev: 38D0
  Type:   Sequential-Access                 ANSI SCSI revision: 03
Attached scsi tape st0 at scsi14, channel 0, id 0, lun 2
st0: try direct i/o: yes (alignment 512 B), max page reachable by HBA 4503599627370495
Attached scsi generic sg7 at scsi14, channel 0, id 0, lun 2,  type 1
scsi scan: INQUIRY to host 14 channel 0 id 0 lun 3
  Vendor: IBM       Model: ULTRIUM-TD2      Rev: 38D0
  Type:   Sequential-Access                 ANSI SCSI revision: 03
Attached scsi tape st1 at scsi14, channel 0, id 0, lun 3
st1: try direct i/o: yes (alignment 512 B), max page reachable by HBA 4503599627370495
Attached scsi generic sg8 at scsi14, channel 0, id 0, lun 3,  type 1
```

This log output shows a controller at LUN 0, the medium changer at LUN 1 and two SCSI tape devices at LUNs 2 and 3. The example below is what the scsi_id call returns:

```
[root@localhost ~]# scsi_id -g -s /class/scsi_tape/nst0
1IBM     ULTRIUM-TD2     1110133831
[[root@localhost ~]# scsi_id -g -s /class/scsi_tape/nst1
1IBM     ULTRIUM-TD2     1110133994
```

Notice that the unique Id is actually comprised of three value with space delimiters. A udev rule must have a unique id for the device, meaning all three parts of this returned string are required. To do this, use the following command.

```
[root@localhost ~]# scsi_id -u -g -s /class/scsi_tape/nst0
1IBM_____ULTRIUM-TD2_____1110133831
[root@localhost ~]# scsi_id -u -g -s /class/scsi_tape/nst1
1IBM_____ULTRIUM-TD2_____1110133994
```

Creating the udev persistent name for SCSI tape has the same process as SCSI disk once the SCSI ID call needed to extract a unique id is known.

Below is the rule for the FC-Tape device:

BUS="scsi", SYSFS{vendor}="HP", SYSFS{model}="ULTRIUM 3-SCSI", PROGRAM="/sbin/scsi_id -p 0x83 -u -g -s /class/scsi_tape/nst%n",RESULT="350060b000029b592", SYMLINK="fc_lun_st%n"

The rule for the FC-SCSI tape device follows:

BUS="scsi", SYSFS{vendor}="IBM", SYSFS{model}="ULTRIUM-TD2", PROGRAM="/sbin/scsi_id -p 0x83 -u -g -s /class/scsi_tape/nst%n",RESULT="1IBM_____ULTRIUM-TD2_____1110133831", SYMLINK="fc_lun_st%n"

BUS="scsi", RESULT="1IBM_____ULTRIUM-TD2_____1110133994", SYMLINK="fc_lun_st%n"

Create a new file named /etc/udev/rules.d/45-local.rules and put the appropriate rule in it. Then run udevtrigger to reload the udev rules.

And finally, here is the output of the rule:

```
[root@localhost ~]# udevtrigger
[root@localhost ~]# ls -al /dev/fc*
lrwxrwxrwx  1 root root 3 Apr  7 15:03 fc_lun_st0 -> st0
lrwxrwxrwx  1 root root 3 Apr  7 15:03 fc_lun_st1 -> st1
```

Further Information About Persistent Names

Refer to the following references for more information on persistent naming:

http://www.kroah.com/linux/talks/ ols_2003_udev_paper/Reprint-Kroah-Hartman-OLS2003.pdf

http://www.reactivated.net/udevrules.php by Daniel Drake (dsd)

http://kernel.org/pub/linux/utils/kernel/hotplug/udev_vs_devfs by Greg Kroah-Hartman

http://linux.dell.com/devlabel/devlabel.html

Performing Diagnostic Tests Using the HBAnyware Utility

Use the Diagnostics tab to do the following:

- Run these tests on Emulex HBA's installed in the system:
  - PCI Loopback (see page 79)
  - Internal Loopback (see page 79)
  - External Loopback (see page 79)
  - Power-On Self Test (POST) (see page 76)
  - Echo (End-to-End) (see page 81)
  - Quick Test (see page 76)
- Perform a diagnostic dump (see page 77)
- View PCI registers and wakeup parameter (see page 78)
- Control HBA beaconing (see page 76)

Note: Diagnostic test functionality is only supported for HBAs that were discovered out-of-band and for HBAs that are installed in the local host.

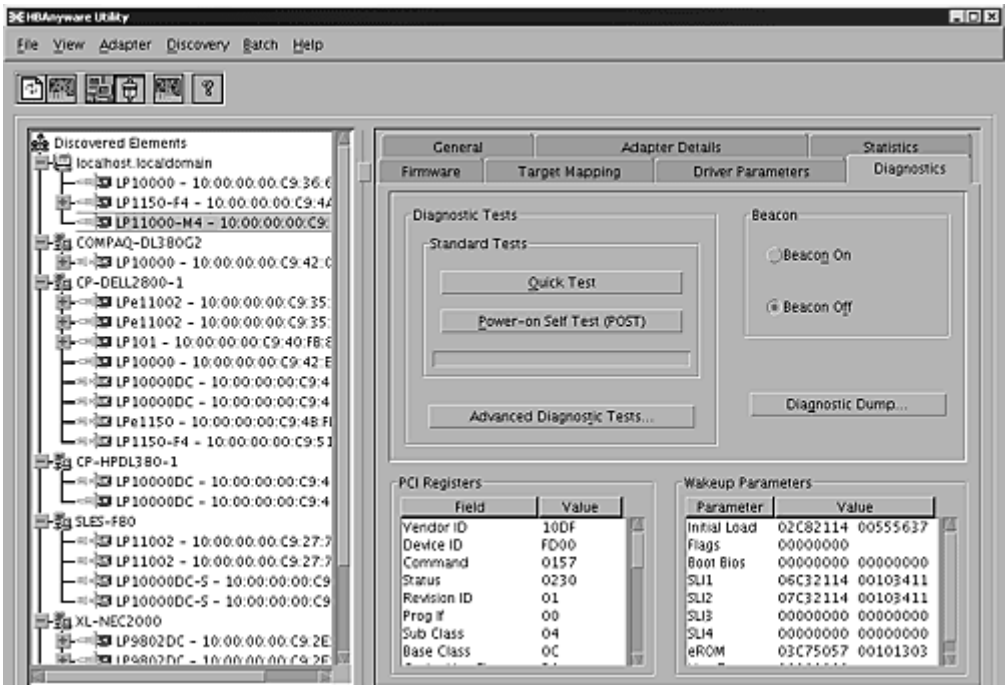


Figure 32: HBAnyware Utility, Diagnostics Tab

All functions are supported locally and remotely, except for the dump feature which is only supported locally.

Running a Quick Test

The Diagnostics tab enables you to run a "quick" diagnostics test on a selected HBA. The Quick Test consists of 50 PCI Loopback test cycles and 50 Internal Loopback test cycles.

To run a quick test:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA on which you wish to run the Quick Test.
3. Select the Diagnostics tab and click **Quick Test**. The following message appears:

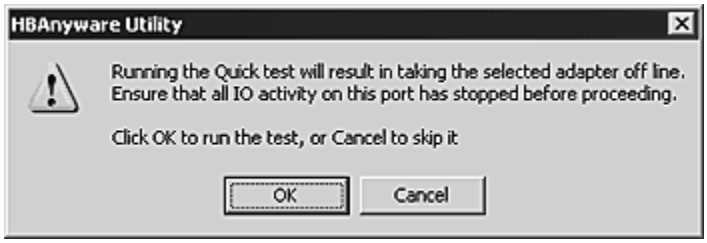

HBAnyware Utility
Running the Quick test will result in taking the selected adapter off line.
Ensure that all IO activity on this port has stopped before proceeding.
Click OK to run the test, or Cancel to skip it
OK
Cancel

Figure 33: HBAnyware Utility, Quick Test Message

4. Click **OK** to run the test. The Quick Diagnostics Test message shows the PCI Loopback and Internal Loopback test results.

Running a POST Test

The POST (Power On Self Test) is a firmware test normally performed on an HBA after a reset or restart. The POST does not require any configuration to run.

To run the POST Test:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA on which you wish to run the POST Test.
3. Select the Diagnostics tab and click **Power-on Self Test (POST)**. A warning dialog box appears.

Figure 34: POST Test Warning window

4. Click **OK**. A POST Test window shows POST test information.

Using Beaconing

The beaconing feature enables you to force a specific HBA's LEDs to blink in a particular sequence. The blinking pattern acts as a beacon, making it easier to locate a specific HBA among racks of other HBAs.

When you enable beaconing, the two LEDs blink rapidly in unison for 24 seconds, after which the LEDs report the HBA health status for 8 seconds. When the 8 seconds are up, the HBA returns to beaconing mode. This cycle repeats indefinitely until you disable this feature or you reset the HBA.

Note: The beaconing buttons are disabled if the selected HBA does not support beaconing.

To enable or disable beaconing:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA whose LEDs you wish to set.
3. Select the Diagnostics tab and click **Beacon On** or **Beacon Off**.

Creating Diagnostic Dumps

The diagnostic dump feature enables you to create a “dump” file for a selected HBA. Dump files contain various information such as firmware version, driver version and so on, that is particularly useful when troubleshooting an HBA.

Note: The Diagnostic Dump feature is only supported for local HBAs. If a remote HBA is selected from the tree-view, the Initiate Diagnostic Dump is disabled.

To start a diagnostic dump:

1. Start the HBAnyware utility.
2. From the discovery-tree, select a local HBA whose diagnostic information you wish to dump.
3. Select the Diagnostics tab and click **Diagnostic Dump**. The Diagnostic Dump dialog box appears. You can specify how many files you want to save using the Files Retained counter. Click **Delete Existing Dump Files** if you wish to remove existing dump files from your system.

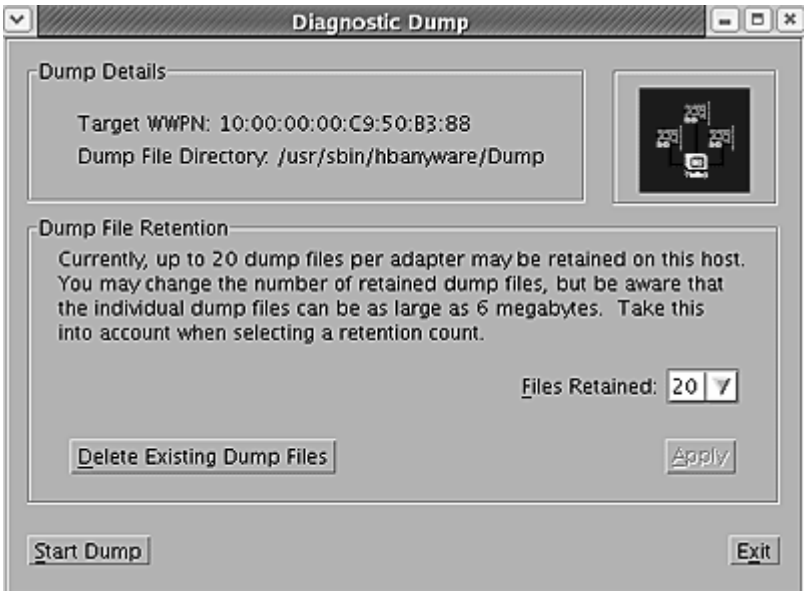

Diagnostic Dump
Dump Details
Target WWPN: 10:00:00:00:C9:50:B3:88
Dump File Directory: /usr/sbin/hbanyware/Dump
Dump File Retention
Currently, up to 20 dump files per adapter may be retained on this host.
You may change the number of retained dump files, but be aware that
the individual dump files can be as large as 6 megabytes. Take this
into account when selecting a retention count.
Files Retained: 20
Delete Existing Dump Files
Apply
Start Dump
Exit

Figure 35: HBAnyware Utility, Diagnostic Dump Dialog Box

4. Click **Start Dump**.

Displaying PCI Registers and Wakeup Information

A PCI Register dump for the selected HBA appears in the lower left panel of the Diagnostics tab. Wakeup information for the selected HBA appears in the lower right panel of the Diagnostics tab. The information is read-only and is depicted below:

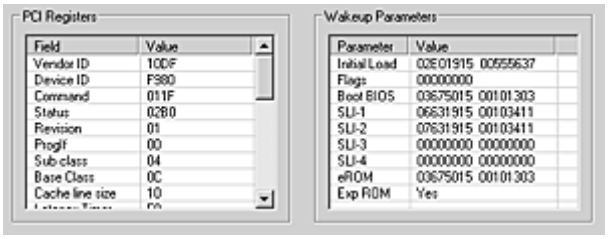


Figure 36: HBAnyware Utility, PCI Registers and Wakeup Parameters Area of the Diagnostics Tab

Running Advanced Diagnostic Tests

The Advanced Diagnostics feature gives you greater control than the Quick Test over the type of diagnostics tests that run. Through Advanced Diagnostics, you can specify which tests to run, the number of cycles to run, and what to do in the event of a test failure.

To run advanced diagnostics tests:

1. Start the HBAnyware utility.
2. Click **Advanced Diagnostics Test** on the Diagnostics tab to view the Advanced Diagnostics dialog box.

   You can run four types of tests:

   - PCI Loopback
   - Internal Loopback
   - External Loopback
   - End-to-End (ECHO)

Note: You cannot run the External Loopback test and ECHO test concurrently. If you select External Loopback the ECHO test section is disabled and vice versa.

All test results, plus the status of running tests, are time stamped and appear in the log at bottom of the dialog box.

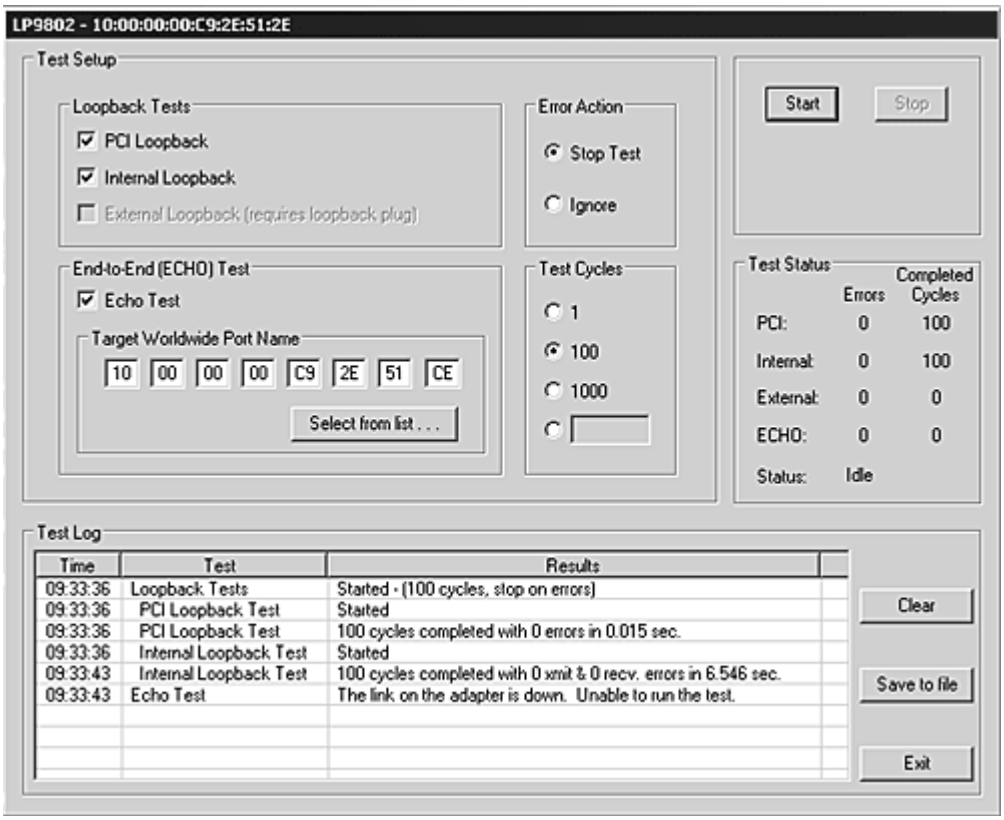


Figure 37: HBAnyware Utility, Advanced Diagnostics

Running Loopback Tests

To run a loopback test, use the "Loopback Test" section of the Advanced Diagnostics dialog box.

You can run the following loopback test combinations using the appropriate check boxes:

- PCI Loopback Test - A firmware controlled diagnostic test in which a random data pattern is routed through the PCI bus without being sent to an adapter link port. The returned data is subsequently validated for integrity.
- Internal Loopback Test - A diagnostic test in which a random data pattern is sent down to an adapter link port, then is immediately returned without actually going out on the port. The returned data is subsequently validated for integrity.
- External Loopback Test - A diagnostic test in which a random data pattern is sent down to an adapter link port. The data goes out the port and immediately returns via a loopback connector. The returned data is subsequently validated for integrity.

Note: You cannot run the External Loopback test and ECHO test concurrently. If you select External Loopback the ECHO test section is disabled and vice versa.

You can specify the number of test cycles by clicking one of the cycle counts values in the "Test Cycles" section of the dialog box or enter a custom cycle count if you wish. The Test Status section displays how many cycles of each test ran. The "Error Action" section of the dialog box enables you to define what should be done in the event of a test failure.

There are two error action options:

- Stop Test - The error will be logged and the test aborted. No further tests will run.
- Ignore - Log the error and proceed with the next test cycle.

To run loopback tests:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA on which you wish to run the Loopback Test.
3. Select the Diagnostics tab and click **Advanced Diagnostics Tests**. From the "Loopback Test" section of the dialog box, choose the type of Loopback test you wish to run and define the loopback test parameters.

   Note: You must insert a loopback plug in the selected HBA before running an External Loopback test.

4. Click **Start**. The following warning appears:

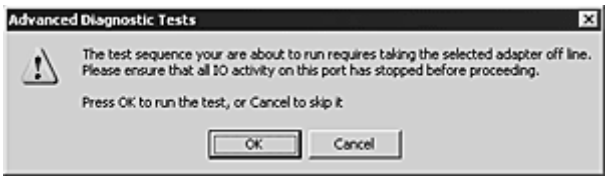

Advanced Diagnostic Tests
The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.
Press OK to run the test, or Cancel to skip it
OK
Cancel

Figure 38: HBAnyware Utility, Advanced Diagnostic Tests Warning

5. Click **OK**. If you choose to run an External Loopback test the following window appears:

Advanced Diagnostic Tests
The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.
The loopback tests you have chosen require that a loopback plug be inserted into the back of the adapter to be tested. Failure to do so can result in the board not returning to an on line state. Please make sure the loopback plug is inserted before pressing the OK button.
Press OK to run the test, or Cancel to skip it
OK
Cancel

Figure 39: HBAnyware Utility, Advanced Diagnostic Tests Warning for External Loopback

6. Click **OK**. The progress bar indicates that the test is running.

   Periodic test feedback, consisting of the current loopback test/cycle plus the completion status of each type of test, is displayed in the "Test Log" section of the dialog box. Click **Clear** to erase the contents of the log display or click **Save to File** to save the log file.

Running End-to-End (ECHO) Tests

Run echo tests using the "End-to-End (ECHO) Test" section of the Diagnostics tab. The end-to-end test enables you send an ECHO command/response sequence between an HBA port and a target port.

Note: Not all remote devices respond to an echo command.

You cannot run the ECHO test and the External Loopback test concurrently. If you select the ECHO Test the External Loopback test is disabled.

To run end-to-end echo tests:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA from which you wish to initiate the End-to-End (ECHO) Test.
3. Select the Diagnostics tab. Click **Advanced Diagnostics Test** (see Figure 40 on page 81).
4. Check **Echo Test**. Enter the World Wide Port Name (WWPN) for the target.

   or

   Click **Select From List** if you do not know the actual WWPN of the test target. The Select Echo Test Target dialog box appears. Select the port you wish to test from the tree-view and click **Select**.

   All relevant information for the selected port is automatically added to the Target Identifier section of the Diagnostics dialog box.

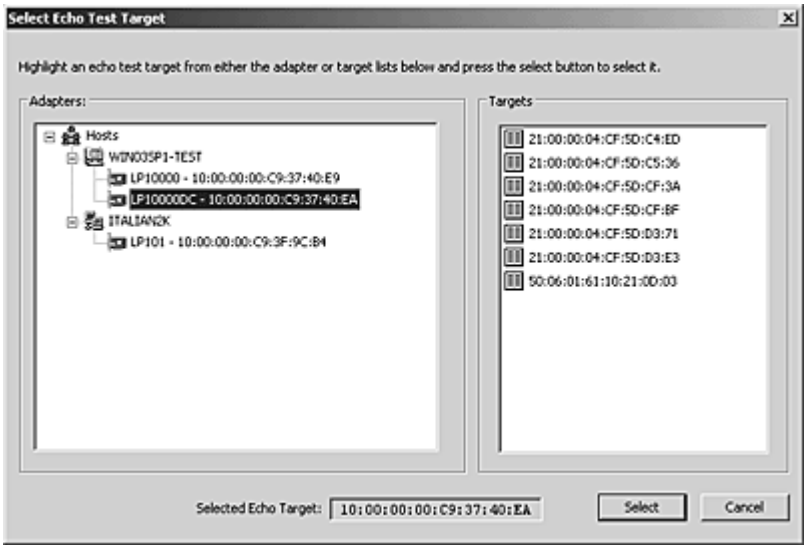


Figure 40: HBAnyware Utility, Select Echo Test Target Window

5. Click **Start**. The following warning window appears:

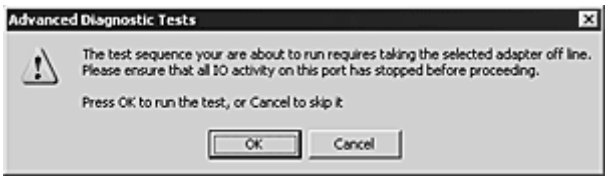

Advanced Diagnostic Tests
The test sequence your are about to run requires taking the selected adapter off line.
Please ensure that all IO activity on this port has stopped before proceeding.
Press OK to run the test, or Cancel to skip it
OK
Cancel

Figure 41: HBAnyware Utility, Advanced Diagnostic Tests Warning

6. Click **OK**. A result screen appears and the test results appear in the Test Log. Click **Clear** to erase the contents of the log display or click **Save to File** to save the log file.

Saving the Log File

You can save the test log to a log file for later viewing or printing. When new data is written to a saved file, the data is appended to the end of the file. Each entry has a two-line header that contains the identifier of the HBA being tested and the date and time of the test. Over time, the data accumulates to form a chronological history of the diagnostics performed on the HBA.

After writing an entry into the log, you are prompted to clear the display.

The default name of the saved file is DiagTestLog.log and by default is located in:
/usr/sbin/hbanyware/Dump

An example of a saved log file appears below:

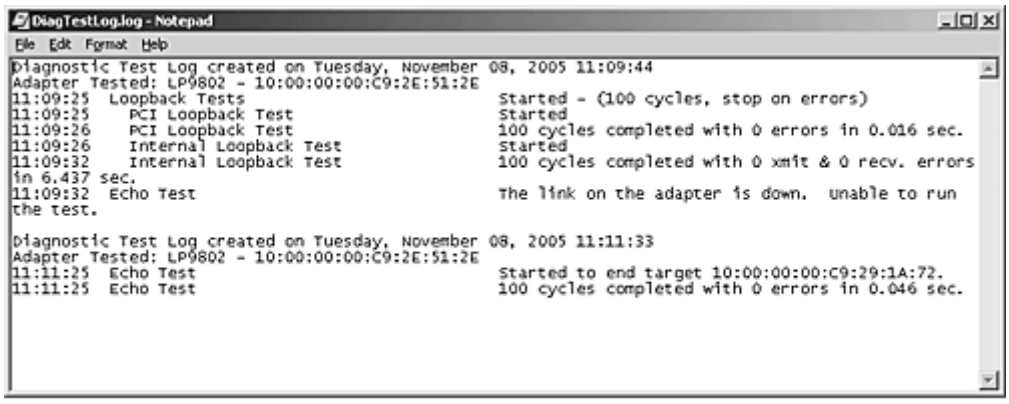

DiagTestLog.log - Notepad
File Edit Format Help
Diagnostic Test Log created on Tuesday, November 08, 2005 11:09:44
Adapter Tested: LP9802 - 10:00:00:00:C9:2E:51:2E
11:09:25 Loopback Tests Started - (100 cycles, stop on errors)
11:09:25 PCI Loopback Test Started
11:09:26 PCI Loopback Test 100 cycles completed with 0 errors in 0.016 sec.
11:09:26 Internal Loopback Test Started
11:09:32 Internal Loopback Test 100 cycles completed with 0 xmit & 0 recv. errors in 6.437 sec.
11:09:32 Echo Test The link on the adapter is down. Unable to run the test.
Diagnostic Test Log created on Tuesday, November 08, 2005 11:11:33
Adapter Tested: LP9802 - 10:00:00:00:C9:2E:51:2E
11:11:25 Echo Test Started to end target 10:00:00:00:C9:29:1A:72.
11:11:25 Echo Test 100 cycles completed with 0 errors in 0.046 sec.

Figure 42: DiagTestLog Window

To save the log file:

1. After running a test from the Diagnostic Test Setup dialog box, Click **Save to File**. The Select Diagnostic Log file Name dialog box appears. The default name of a saved file is DiagTestLog.log.
2. Browse to the desired directory, change the log file name if you wish and click **Save**.

Out-of-Band SAN Management

Out-of-Band (OOB) remote SAN management is achieved by sending the remote management requests over a LAN using the Ethernet TCP/IP protocol to remote hosts.

In-band management is achieved by sending the remote management requests over a SAN to remote hosts.

The principle differences between in-band and out-of-band SAN Management are:

- A management host with an HBA installed does not need to connect to a fabric to manage other hosts.
- An OOB management host can manage all of the HBAs in a remote host, not just the ones connected to the same fabric. In-band can only manage HBAs connected to the same fabric.
- You can manage many more hosts since OOB is not constrained by the boundaries of a fabric or zoning.
- True board status (e.g. link down) is available since the in-band path is not necessary to send a status request to the remote host.
- HBA security in an OOB environment is much more important since many more hosts are available for management and OOB access is not affected by fabrics or zoning.
- Discovery of hosts in an OOB environment is much more difficult than in-band discovery.

Adding a Single Host

The HBAnyware utility enables you to specify a single OOB host to manage. If the host is successfully discovered as a manageable host, it is added to the static list of hosts and if it has not been discovered in-band, the host and its HBAs are added to the discovery tree.

To add a single host:

1. Start the HBAnyware utility.
2. From the Discovery menu, select **Out-of-Band/Add Host**. The Add Remote Host dialog box appears.

Figure 43: HBAnyware Utility, Add Remote Host Dialog Box

3. Enter the name or the IP address of the host to be added. Entering the IP address is the best way to add a new host.

Note: Using the IP address to identify the host avoids name resolution issues.

4. Click **OK**. You will receive a message indicating whether or not the new host was successfully added.

Adding a Range of Hosts

You can find the OOB manageable hosts by searching a range of IP addresses using the Add Range of IP Hosts dialog box.

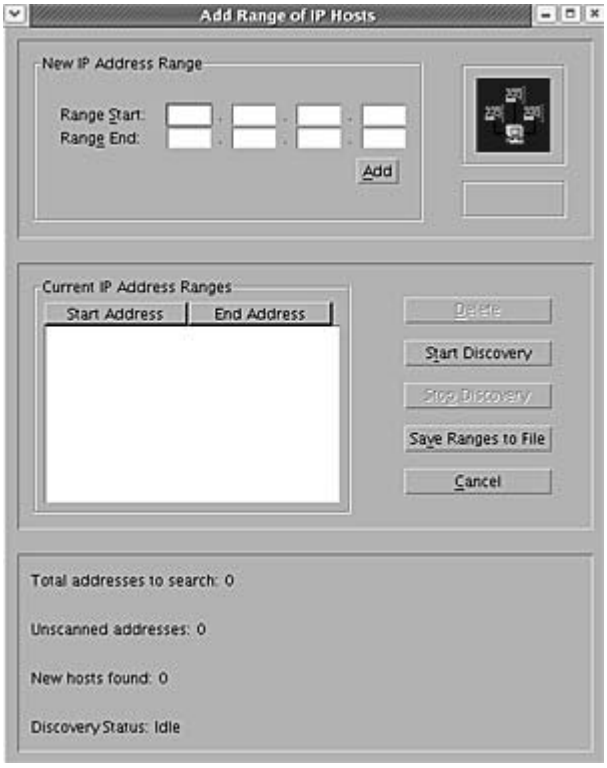


Figure 44: HBAnyware Utility, Add Remote Hosts Window

The Add Range of IP Hosts dialog box enables you to build the initial list of OOB manageable hosts.

To add a range of hosts:

1. Start the HBAnyware utility.
2. From the Discovery menu, select **Out-of-Band/Add Range of Hosts**. The Add Range of IP Hosts dialog box appears.
3. Enter the complete start and end address range and click **Add**. The added address range appears in the dialog box. Add any additional ranges you wish to search.

4. Click **Start Discovery**. The HBAnyware utility checks each address in the range to determine if the host is available and remotely manageable. The number of addresses discovered (of manageable hosts) is periodically updated on the dialog box.

Note: The number of addresses does not correspond directly to the number of hosts added to the discovery-tree.

For example, some of the addresses discovered may be for hosts that have already been discovered in-band. However, new HBAs may be discovered on those hosts that were not discovered in-band.

Also, a host may have more than one HBA installed and both IP addresses for that host are discovered during the search, but only one host will possibly be added to the discovery-tree.

---

5. When the search is complete, click **Cancel**.
6. A dialog box appears asking to save the IP ranges you searched. Click **Yes** to save the address ranges. If you save the address ranges, these address ranges will appear the next time you use the Add Range of IP Hosts dialog box. Click **No** if you do not want to save the address ranges.

The **Save Ranges to A File** button saves the specified range(s) to a file so that the same ranges can be automatically invoked when the HBAnyware utility is started again.

Removing Hosts

Periodically you may want to remove hosts that are no longer part of the network. You may want to remove a host when it is removed from the network or to detect hosts that are no longer being discovered. Removing hosts that can no longer be discovered improves the operation of the discovery server.

To remove hosts:

1. Start the HBAnyware utility.
2. From the Discovery menu, select **Out-of-Band/Remove Host**. The Remove Remote Hosts dialog box shows a list of discovered OOB hosts. Any host not currently discovered appears in red. Click **Show Undiscovered Hosts Only** to only display currently undiscovered hosts.
3. From the Remove Remote Hosts dialog box, select the hosts you wish to remove. You can select all the displayed hosts by clicking **Select All**.
4. Click **OK** to remove the selected hosts.

HBAnyware Security

Introduction

After you install the base HBAnyware software, which includes the HBAnyware utility and remote server, on a group of systems, the HBAnyware utility on any of those systems can remotely access and manage the HBAs on any systems in the group. This may not be a desirable situation, because any system can perform actions such as resetting boards or downloading firmware.

You can use the HBAnyware utility security package to control which HBAnyware enabled systems can remotely access and manage HBAs on other systems in a Fibre Channel network. HBAnyware security is systems-based, not user-based. Anyone with access to a system that has been granted HBAnyware client access to remote HBAs can manage those HBAs. Any unsecured system is still remotely accessible by the HBAnyware client software (HBAnyware utility).

The HBAnyware security software provides two main security features:

1. Prevent remote HBA management from systems that you do not want to have this capability.
2. Prevent an accidental operation (such as firmware download) on a remote HBA. In this case, you do not want to have access to HBAs in systems you are not responsible for maintaining.

The first time you run the HBAnyware Security Configurator on a system in an environment where no security as been configured, the initial Access Control Group (ACG) is created. At this point, only this system has remote access to the HBAs in the systems in the ACG. They are no longer remotely accessible from any other system.

Subsequently, you can create additional Access Sub-Groups (ASGs). This grants systems in the ACG the ability to remotely access the HBAs of other selected systems in the ACG.

Starting the HBAnyware Security Configurator

Prerequisites

Before you can start the HBAnyware Security Configurator, you must have the following items installed on your system:

- The Emulex driver for Linux
- The HBAnyware and lputil Utilities
- The HBAnyware Security Configurator

Note: Before you start the Configurator, you must make sure that all of the systems that are part of, or will be part of, the security configuration are online on the network so that they receive updates or changes made to the security configuration.

Any system that is already part of the security installation might not run with the proper security attributes, if updates to the security configuration are made while it is offline.

Any system that is part of the security installation and that is offline when the HBAnyware Security Configurator starts will not be available for security configuration changes even if it is brought online while the Configurator is running.

Procedure

To start the HBAnyware Security Configurator:

1. Run the /usr/sbin/hbanyware/ssc script. Type:

   ```
   /usr/sbin/hbanyware/ssc
   ```

Running the Configurator for the First Time/Creating the ACG

When you install the HBAnyware utility Security software on a system and run the HBAnyware utility Security Configurator for the first time, that system becomes the Master Security Client (MSC). All of the available servers are discovered and are available to be part of the system Access Control Group (ACG). You select the systems to add to the ACG, and the security configuration updates on all of the selected servers as well as on the initial system. This selection constitutes the participating platforms in this security installation.

To create the ACG:

1. Start the HBAnyware utility Security Configurator for the first time in an unsecure environment. The following message appears:

HBAnyware Security Configurator
This utility is running on an unsecure system. Continuing will allow you to set up a new security configuration making this system the Master Client System.
OK
Cancel

Figure 45: HBAnyware Security Configurator "Unsecure System" message

2. Click **OK**. The Access Control Group tab appears:

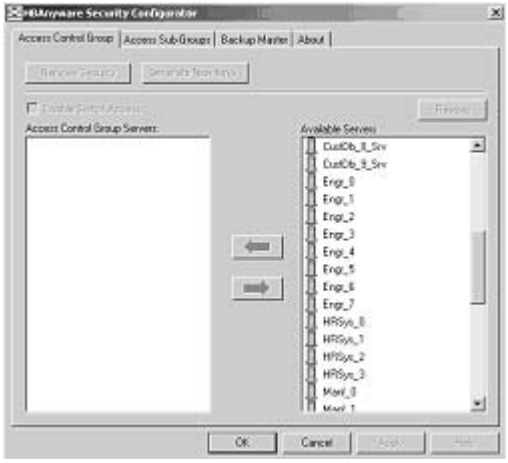


Figure 46: HBAnyware Security Configurator, Access Control Group Tab - No ACG Servers

3. Select the unsecured servers that you want to add to the ACG from the Available Servers list.

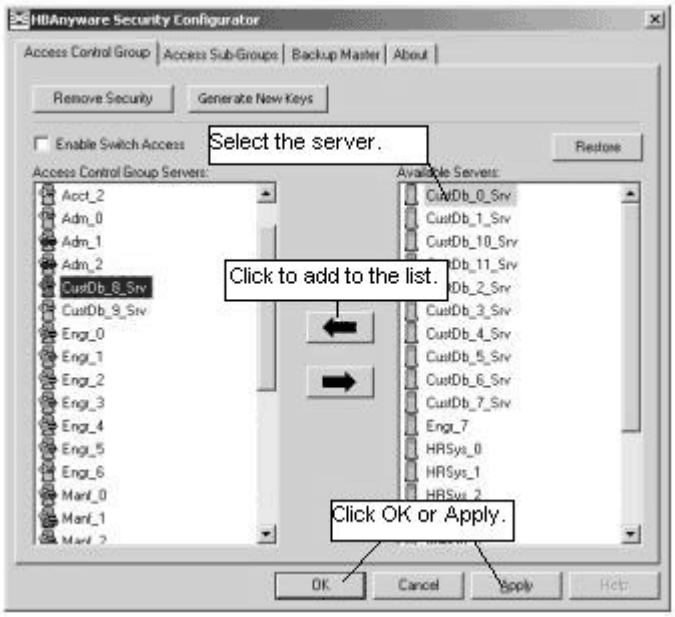


Figure 47: HBAnyware Security Configurator, Access Control Group Tab with ACG Servers

4. Click the **left arrow** to add the servers to the Access Control Group Servers list.
5. Click **OK** or **Apply**.

Designating a Master Security Client

The first time you run the HBAnyware Security Configurator on any system in a Fibre Channel network, that system becomes the MSC (Master Security Client). See “Running the Configurator for the First Time” on page 87 for more information.

Access Control Groups

Introduction

The Access Control Group tab shows the systems that are part of a client's Access Control Group (ACG) and, from the Master Security Client (MSC), allows you to select the systems that belong to the ACG.

Access Control Group Tab on the MSC

On the MSC, you select or deselect the systems that are to be part of the security installation in the Access Control Group tab. When you select unsecure systems and move them to the Access Control Group Servers list, these systems updates to secure them and bring them into the MSC's ACG. When

you select systems in the ACG and move them to the Available Servers list, the security configuration for those systems update to make them unsecure. After you have configured security from the MSC for the first time, the Access Control Group tab looks similar to the following:

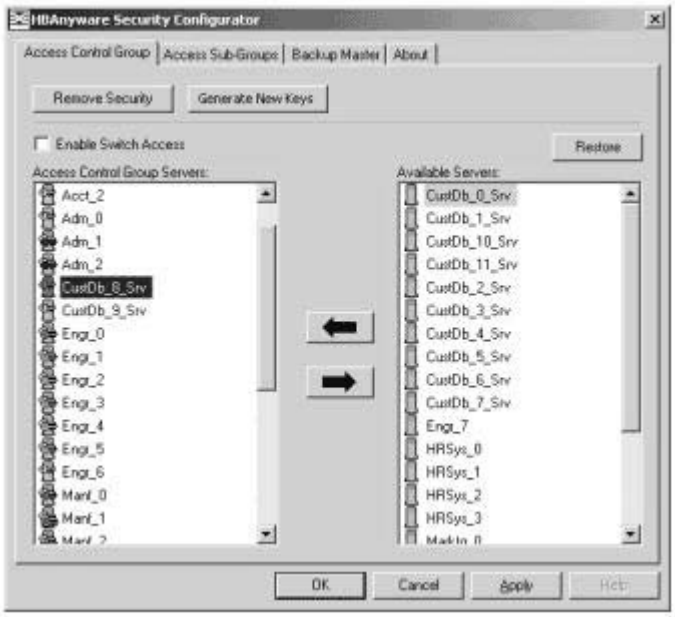


Figure 48: HBAnyware Security Configurator, Access Control Group Tab on an MSC System

Access Control Group Tab on a Non-MSC

On a non-MSC system, the Access Control Group tab shows the systems that are part of the client's ACG. You cannot modify the ACG on a non-MSC. (You can modify the ACG only on the MSC or a client higher in the security topology's hierarchy.) The ACG tab on a non-MSC system looks similar to the following:

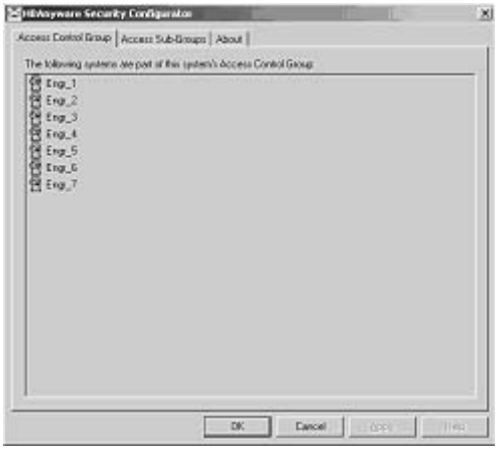


Figure 49: HBAnyware Security Configurator, Access Control Group Tab on a Non_MSC System

ACG Icons

Depending on the configured security topology, a system can be a server in one or more ACGs. It can also be a client to an ACG. The following icons indicate the state of each of the systems in the Access Control Group Servers list.

The system is a secure server in the ACG. It does not belong to an Access Sub-Group (ASG). You can remove this system from the ACG.

The system is a secure server in the ACG and belongs to one or more ASGs. You can remove this system from the ACG.

The system is a secure server in the ACG and a client to an ASG. You cannot remove this system from the ACG until you remove it as a client from the ASG.

The system is a secure server in the ACG, a secure server in one or more ASGs and a client to an ASG You cannot remove this system from the ACG until you remove it as a client from the ASGs.

The system is a Backup Master. You cannot remove this system from the ACG until you remove it as a Backup Master.

Run the Configurator for the First Time/Create the ACG

When you install the HBAnyware Security software on a system and run the HBAnyware Security Configurator for the first time, that system becomes the Master Security Client (MSC). All of the available servers are discovered and available to become part of the system Access Control Group (ACG). Select the systems to add to the ACG, and the security configuration updates all of the selected servers as well as on the initial system. This selection constitutes the participating platforms in this security installation.

To create the ACG:

1. Start the HBAnyware Security Configurator for the first time in an unsecure environment. The computer from which you run the Configurator becomes the MSC. The “Unsecured System” message appears (see Figure 45).
2. Click **OK.** The Access Control Group tab appears (Figure 46).
3. Select the unsecured servers that you want to add to the ACG from the Available Servers list (Figure 48).
4. Click the **left arrow** to add the servers to the Access Control Group Servers list.
5. Click **OK** or **Apply**.

Adding a Server to the ACG

After you create the initial Access Control Group (ACG) on the Master Security Client (MSC), you may add unsecured servers to the ACG.

To add servers to the ACG:

1. Start the HBAnyware Security Configurator.
2. On the Access Control Group tab, from the Available Servers list, select the unsecured servers to add to the ACG (Figure 48).
3. Click the **left arrow** to add the server to the Access Control Group Servers list.
4. Click **OK** or **Apply**.

Deleting a Server from the ACG

To delete a server from the Access Control Group (ACG):

1. Start the HBAnyware Security Configurator.
2. On the Access Control Group tab, from the Access Control Group Servers list, select the secured systems to delete from the ACG (Figure 48).
3. Click the **right arrow** to remove the servers from the Acces Control Group Servers list.
4. Click **OK** or **Apply**.

Removing Security from all Servers in the ACG

You can remove security from all systems only from the Master Security Client (MSC). Removing the entire security topology on all of the servers in the MSC's ACG puts the servers in an unsecure state. The MSC is also put in an unsecure state; consequently, it is no longer the MSC. Any participating systems that are not online will not receive the 'remove security' configuration update, and as a result will no longer be accessible remotely.

To remove security from all servers in the ACG:

1. Start the HBAnyware Security Configurator. The Access Control Group tab appears (Figure 48).
2. On the Access Control Group tab, click the **Remove Security** button. The following message appears:

HBAnyware Security Configurator
You are about to remove the security configuration. This means all HBAs will be available to be managed by any other system. This action will be immediate and cannot be reversed. Are you sure you want to do this.
Yes
No

Figure 50: HBAnyware Security Configurator, “Warning” Dialog Box

3. Click **Yes**. Security is removed from all servers in the ACG.

Generating New Security Keys

You can generate new security keys only from a Master Security Client (MSC). After the new security keys are generated, they are automatically sent to all of the remote servers in the Access Control Group (ACG).

Note: All the servers that are part of the ACG must be online when this procedure is performed so that they may receive the new keys. Any servers that do not receive the new keys will no longer be accessible remotely.

To generate new security keys for all servers in the ACG:

1. From the MSC, start the HBAnyware Security Configurator. The Access Control Group tab appears (see Figure 47 on page 88).
2. On the Access Control Group tab, click the **Generate New Keys** button. A dialog box warns you that you are about to generate new security keys for all systems.
3. Click **Yes**. The new keys generate and are sent to all of the remote servers in the ACG.

Restoring the ACG to Its Last Saved Configuration

You can restore the ACG to its last saved configuration, if there are unsaved changes to the ACG, only from the Master Security Client (MSC).

To restore the ACG to its last saved configuration:

1. From the Access Control Group tab on the MSC, click the **Restore** button (Figure 48).

Accessing a Switch

You can enable switch access only on a Master Security Client (MSC). Switch access grants the client access rights to a switch to remotely access HBAs on servers in the Access Control Group (ACG).

To enable switch access:

1. Start the HBAnyware Security Configurator.
2. From the Access Control Group tab, check **Enable Switch Access**. (Figure 48).

Access Sub-Groups

Introduction

Use the Access Sub-Group tab to create multiple Access Sub-Groups (ASGs) and multiple levels (tiers) in the security topology hierarchy. The hierarchy can be as many levels deep as desired. However, we recommend the hierarchy extend no more than three levels deep, as it becomes increasingly difficult to keep track of the topology the deeper it goes. The hierarchy shows in the Access Sub-Groups tab as a tree. You can create, modify and delete ASGs at each level in this tree.

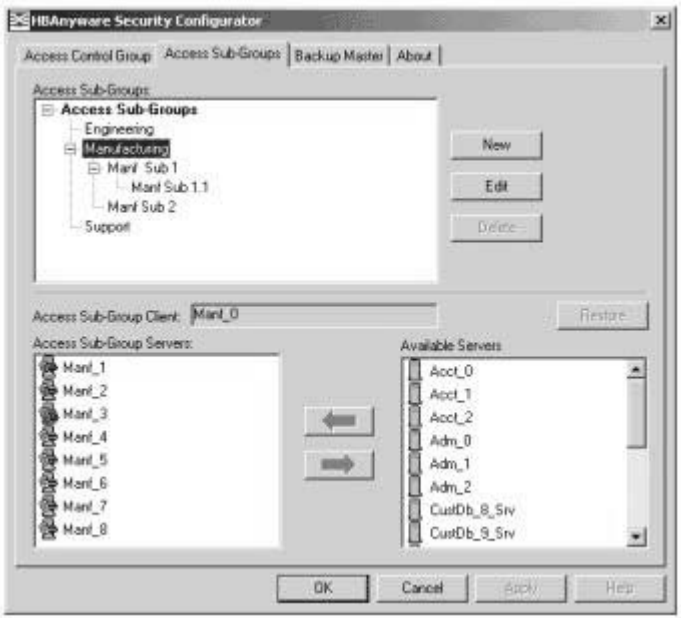


Figure 51: HBAnyware Security Configurator, Access Sub-Groups Tab with Sub-Groups Created

ASG Icons

The following icons indicate the state of each of the servers in the Access Sub-Group Servers list.

The system is a server in the ASG but not in any child ASGs. You can remove it from the ASG.

The system is a server in the ASG and at least one child ASG. You cannot remove it from the ASG until you remove it from the child ASGs.

The system is a server in the ASG and a client to a child ASG. You cannot remove it from the ASG until you remove it as a client from the child ASG (by either deleting or editing the child ASG).

The system is a server in the ASG, a server in at least one other child ASG and a client to a child ASG. You cannot remove it from the ASG until you remove it from the child ASGs and as a client from the child ASG (by either deleting or editing the child ASG).

The system is a server in the ASG and a client to a non-child ASG. You can remove it from the ASG.

The system is a server in the ASG, a server in at least one child ASG, and a client to a non-child ASG. You cannot remove it from the ASG until you remove it from the child ASGs.

Creating an ASG

Create a new Access Sub-Group (ASG) by selecting one system from the Access Control Group (ACG) to be the client, and some or all of the other systems to be servers to this client, thus defining the new client's ACG. When the HBAnyware Security Configurator is run on the new client, the ACG shows the servers that were configured in the ASG by its parent client.

To create an ASG:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Groups tab.

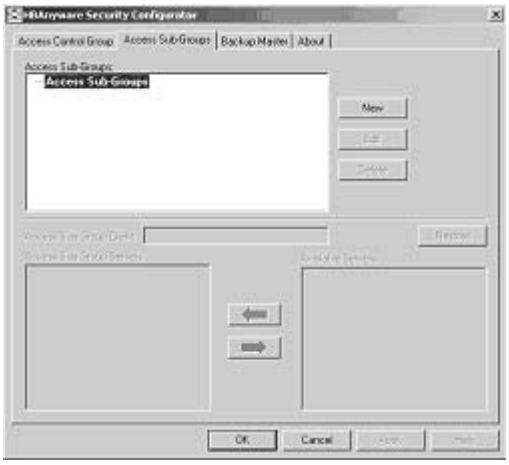


Figure 52: HBAnyware Security Configurator, Access Sub-Groups Tab with No Sub-Groups Created

3. Click **New**. The New Access Sub-Group dialog box appears:

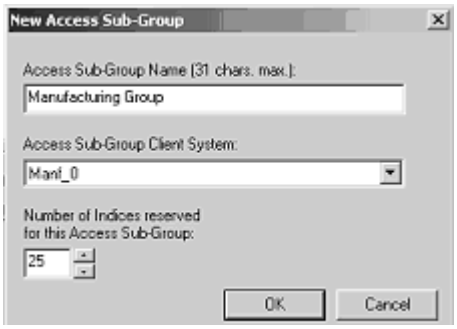


Figure 53: HBAnyware Security Configurator, New Access Sub-Group Dialog Box

4. Enter the ASG information:
    - Access Sub-Group Name: Enter the name of the ASG. The ASG name is for identification purposes only. It does not provide any security function. Provide a name that will make it easy to remember the systems that are part of the ASG. The name can contain any alphanumeric characters, symbols or spaces (up to 31). At each level of the security topology, each ASG name must be unique. If the name is not unique at its level, an error message informs you of this when you click **OK**.
    - Access Sub-Group Client System: Select the system that is to be the client.
    - Number of indices reserved for this Access Sub-Group: Select the number of 'indices' you want to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create on the new client's system.
5. Click **OK** in the New Access Sub-Group dialog box. The ASG is created.

Reserved Indices - Examples

A particular security installation can support the creation of several hundred access groups (ACGs and ASGs). When you create each new access group, you allocate some number of 'indices' to the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create at the new client's system.

- If zero indices are reserved, you cannot create any lower-level ASG under the client of the new ASG. Thus, for example, if you want to implement a multi-tiered security architecture consisting of many ASGs, and you want to create them all from the Master Security Client (MSC), zero indices would be allocated to each of the new ASGs client platforms when they are created.
- If you create an ASG, and you reserve 25 indices for the new ASG client platform, a child ASG created by this platform will have a maximum of only 24 indices available to be reserved (one is taken by the creation of the child ASG itself). This continues down the ASG hierarchy as each lower level ASG is created.
- When you create an ASG from the MSC, a maximum of 50 indices (or less if fewer are available) can be reserved. For all other clients, the maximum depends on how many indices were reserved to that client when its ASG was created, and on how many it has subsequently allocated to its ASGs.

Adding a Server to an ASG

To add a server to an ASG:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Group tab (see Figure 52 on page 93).

3. The name of the ASG appears in the Access Sub-Groups tree. From the Available Servers list, select the servers to add to the ASG.

   Note: Out-of-band servers will appear in the Available Servers list even though the ASG client system may not have discovered them yet. These servers can still be added to the Access Sub-Group Servers list.

4. Click the **left arrow** to move the servers to the Access Sub-Group Servers list.
5. Click **OK** or **Apply** to update servers, adding them to the ASG. The new client can remotely manage the HBAs on those servers using the HBAnyware utility.

Deleting an ASG

Only a leaf node ASG may be deleted (i.e. not ASGs underneath it in the tree). If an ASG has at least one child ASG, you must delete those child ASGs first.

To delete an ASG:

1. From the Access Sub-Group tree, select the leaf node ASG you wish to delete.
2. Click the **Delete** button. A dialog box appears warning you that if you continue the access sub-group will be deleted.
3. Click **Yes**. This operation is immediate. There is no need to click the **OK** or **Apply** button under the tab.

Restoring an ASG to Its Last Saved Configuration

You can restore an Access Sub-Group (ASG) to its last saved configuration if there are unsaved changes to it.

To restore an ASG to its last saved configuration:

1. Click the Access Sub-Group tab (see Figure 52 on page 93).
2. Select the ASG whose configuration you want to restore.
3. Click **Restore**.
4. Click **OK** or **Apply** to save your changes.

Editing an ASG

You can change the name, client system or reserved indices of an Access Sub-Group (ASG).

To edit an ASG:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Group tab (see Figure 52 on page 93).
3. Select the ASG you want to edit.

4. Click **Edit**. The Edit Access Sub-Group dialog box appears:.

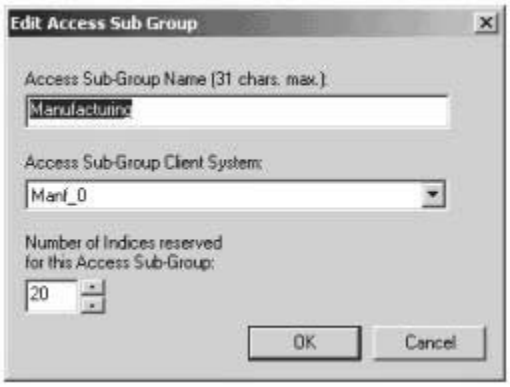


Figure 54: HBAnyware Security Configurator, Edit Access Sub Group Dialog Box

5. Change the ASG information:
   - Access Sub-Group Name: Change the name of the ASG. The ASG name is for identification purposes only. It does not provide any security function. Provide a name that is easy to remember the systems that are part of the ASG.

     The name can contain any alphanumeric characters, symbols or spaces (up to 31). At each level of the security topology, each ASG name must be unique. If the name is not unique at its level, an error message informs you of this when you click **OK**.
   - Access Sub-Group Client System: Select the new system to be the client. If the Configurator is running on a system connected to more than one fabric, the client list contains only those systems that can be accessed by the original client of the ASG.
   - Number of indices reserved for this Access Sub-Group: Select the new number of 'indices' to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create on the new client's system. See page 94 for examples.
6. Click **OK** in the Edit Access Sub-Group dialog box to save your changes.

About Offline ASGs

Sometimes a client system may not be online when the HBAnyware Security Configurator is running. In this case, the Access Sub-Group (ASG) for the client appears offline in the ASG tree, much like the following:

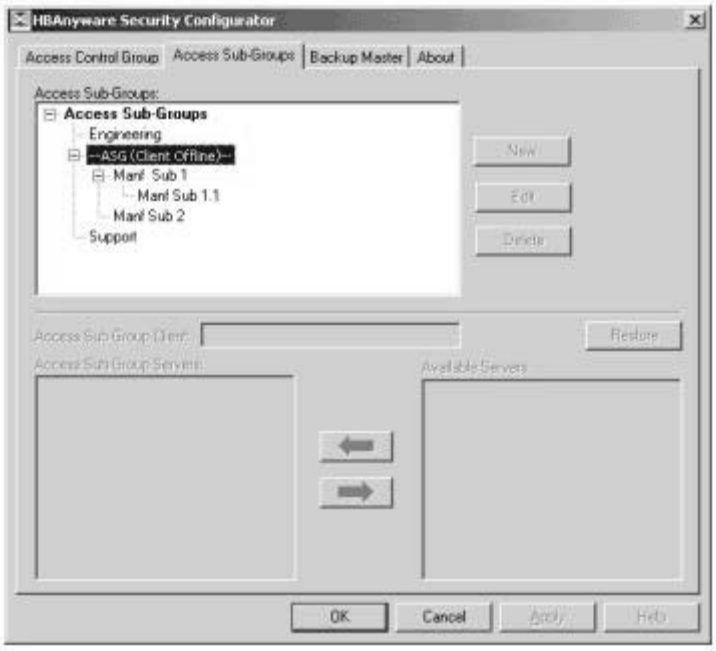


Figure 55: HBAnyware Security Configurator, Access Sub-Groups Tab - Client System Offline

The offline ASG entry serves as a placeholder for where the real ASG would be in the tree. You cannot modify or delete the entry (although it is removed from the display if all of its child ASGs are deleted).

It is possible to delete the child ASGs of an offline ASG. However, we recommend that you delete them only if the client for the offline ASG will never be put online again. It is best to delete child ASGs when the parent ASG is online.

If you choose to delete a child ASG, the operation is immediate. There is no need to click **OK** or **Apply**.

Backup Masters

Introduction

A Backup Master mirrors the security data of the Master Security Client (MSC) in case it has to take over as the MSC if the MSC is unable to operate or is removed from the security configuration. A Backup master system receives all the updates to the security configuration on the MSC. However, you cannot make modifications to the security configuration on a Backup Master.

When the Configurator runs on a Backup Master, the Access Control Group tab looks like the tab on a non-MSC system. The Access Sub-Group tab shows the ASGs, but you cannot change the ASGs (see Figure 48 on page 89).

The Backup Master tab is available only when the HBAnyware Security Configurator is running on the MSC or a Backup Master. Use this tab to set up a system as a Backup Master to the MSC and to replace the MSC with a Backup Master.

Each time you start the HBAnyware Security Configurator on the MSC and no Backup Master is assigned, a message warns you that no Backup Master Client is assigned to the security configuration.

If you run the HBAnyware Security Configurator on a Backup Master, a message warns you that you can only view security information on a Backup Master. Security changes must be made to the MSC.

A Backup Master system receives all the updates that the MSC makes to the security configuration, therefore it is very important that the Backup Master is online when the HBAnyware Security Configurator is running on the MSC. Otherwise, updates to the security configuration are not reflected to the Backup Master. If the Backup Master then becomes the MSC, the security configuration may be corrupted.

Backup Master Eligible Systems

To be eligible to become a Backup Master, a system must not be a client or server in any ASG. In other words, it must be either a server in the MSC's Access Control Group (ACG) or an unsecure system. If it is an unsecure system, it will be secure when it becomes a Backup Master.

Backup Master Tab and Controls

The first time you select the Backup Master tab on the MSC, it looks similar to the following:

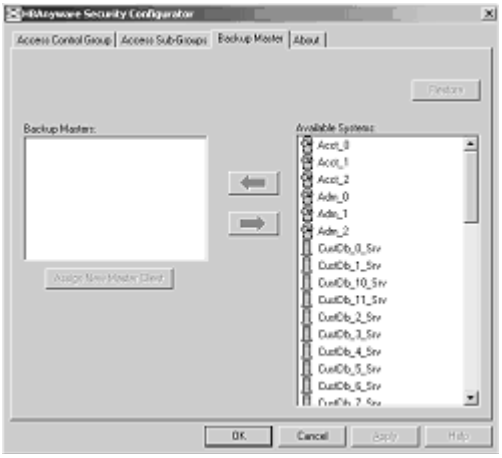


Figure 56: HBAnyware Security Configurator, Backup Master tab - First Time Selected

Creating a Backup Master

To create a Backup Master:

1. On the Master Security Client (MSC), start the HBAnyware Security Configurator.

2. Click the Backup Master tab.

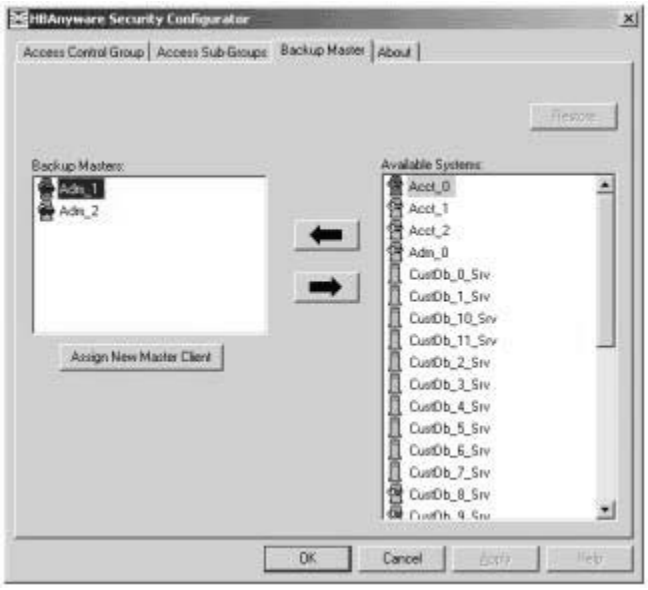


Figure 57: HBAnyware Security Configurator, Backup Master Tab with Backup Masters

3. Select a system from the Available Systems list.
4. Click the **left arrow** to move the system to the Backup Masters list.
5. Click **OK** or **Apply** to save your changes.

Reassigning a Backup Master as the New MSC from the Old MSC

Because a Backup Master may have to take over as the Master Security Client (MSC), it should be able to physically access all of the HBAs that the MSC can access. If the MSC connects to multiple fabrics, select its Backup Master from the Available Systems list connected to the same fabrics as the MSC.

To reassign a Backup Master as the new MSC from the old MSC:

1. On the MSC, start the HBAnyware Security Configurator.
2. Click the Backup Master tab (see Figure 57)
3. In the Backup Masters list, select the Backup Master system that you want to reassign as the MSC.
4. Click **Assign New Master Client**. A dialog box appears and asks if you want to proceed.
5. Click **Yes** on the dialog box. The selected Backup Master becomes the new MSC. The current MSC becomes a server in the new MSC's ACG. After the changes are made, a message indicates that the reassignment is complete.
6. Click **OK**. The Configurator closes because the system is no longer the MSC.

Reassigning a Backup Master as the New MSC from the Backup Master

WARNING: Use this method only if the MSC cannot relinquish control to a Backup Master. For example, if you can no longer boot the MSC or connect to the Fibre Channel network. Under any other circumstances, if the Backup Master takes over as the MSC, and the MSC is still running or comes back online later, there will be two MSCs for the same security configuration. This will eventually lead to corruption of the security configuration.

To reassign a Backup Master as the new MSC from the Backup Master:

1. On the Backup Master system that you want to reassign as the MSC, start the HBAnyware Security Configurator.
2. Click the Backup Master tab.

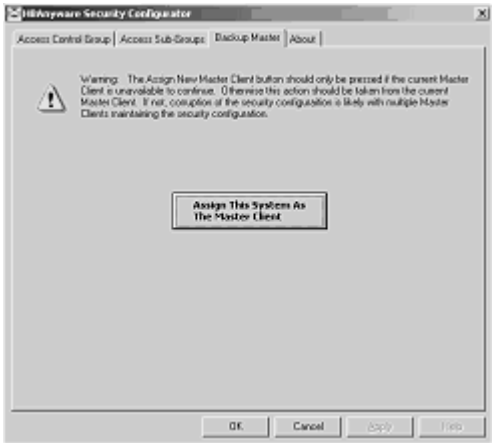


Figure 58: HBAnyware Security Configurator, Backup Master "Warning" Dialog Box

3. Click **Assign This System As The Master Client**. A prompt asks if you want to continue.
4. Click **Yes**. A prompt notifies you that this system is now the new MSC.
5. Click **OK**. The Configurator closes.
6. Restart the HBAnyware Security Configurator to run the former Backup Master as the MSC.

Troubleshooting

Introduction

There are several circumstances in which your system may operate in an unexpected manner. The Troubleshooting section explains many of these circumstances and offers one or more workarounds for each situation.

Unusual Situations and their Resolutions

General Situations

Table 5: General Driver and HBAnyware Situations

Situation	Resolution
When attempting to start HBAnyware the Web browser displays "Emulex Corporation HBAnyware Demo of HBAnyware WebStart web n.n.n.n ..."	The document caching mechanism sometimes behaves erratically if more than one version of Java Runtime is installed on the browser client. There are two workarounds for this problem: • Exit the browser and restart it. HBAnyware with Web launch should start successfully. • Uninstall all non-essential versions of the Java Runtime. HBAnyware Web Launch services require that only a single version of the Java Runtime be installed on the browser client. This single version should be JRE version 1.5 or greater.
If a SAN configuration has 256 targets mapped by the lpfc driver, any additional added targets do not get a target ID mapping by the driver and cause target discovery to fail. Removing targets or reinitializing the link does not solve the problem.	Unload and reload the driver to reset available target IDs. Ensure that the SAN configuration is correct prior to rebooting the driver. This will clear the driver's consistent binding table and free target IDs for new target nodes.
In some cases, after loading an OEM supplied combined firmware/OpenBoot image you will not be able to enable BootBIOS from the lputil Boot BIOS Maintenance menu. Should you encounter this problem after loading the OEM combined firmware/ OpenBoot image, follow the steps outlined in the resolution.	1. Download the current OpenBoot only image for your adapter from the Emulex Web site. 2. Load the current OpenBoot only image following steps listed in Updating BootBIOS section of this manual. 3. Run lputil, return to Boot BIOS Maintenance menu. 4. Enable BootBIOS.
rmmod fails to unload lpfc driver module due to ERROR: Module lpfc is in use. This message can appear when you attempt to remove the driver and there is a Logical Volume Group dependent on the driver.	Make the Logical Volume Group unavailable. Type: lvchange -a n xxxxxxx where xxxxxx is the Volume Group Name.

Table 5: General Driver and HBAnyware Situations (Continued)

Situation	Resolution
LP1005DC-CM2 reported as the LP1050DC. When running lspci or kudzu utilities, you may see the Emulex FC Host Adapter LP1005DC-CM2 reported as the Emulex FC Host Adapter LP1050DC for the pci_id address f0a5. This is due to a delay in getting the pci_id tables updated in the Linux distributions.	None at this time.
An lspci will show recent Emulex HBAs as "unknown". This is because of the delay of getting new product ID's into the Linux development cycle.	None at this time.
Slow targets or extended link faults on the storage side may result in storage being marked off-line by the mid-layer and remaining off-line (not recovered) when the link faults are corrected.	This version of the driver should eliminate this problem. However, should you experience off-line device issues, increase the SCSI command timeout to a value greater than or equal to sixty seconds. Emulex also provides a script which addresses this issue (for 2.6 kernels). Go to: www.emulex.com/ts/downloads/linuxfc/linux.html and click the Linux tools link to access the lun_change_state.sh script.
Under certain conditions of an I/O load, some targets cannot retire an I/O issued by a Linux initiator within the default timeout of 30 seconds given by the scsi midlayer. If the situation is not corrected, the initiator-to-target condition deteriorates into abort/recovery storms leading to I/O failures in the block layer. These types of failures are preceded by a SCSI IO error of hex 6000000.	Emulex provides a script which addresses this issue. Go to: www.emulex.com/ts/downloads/linuxfc/linux.html and click the Linux tools link to access the set_target_timeout.sh script.
lpfc driver fails to recognize an HBA and logs "unknown IOCB" messages in the system log during driver load. The HBA is running outdated firmware.	Upgrade HBA firmware to minimum supported revision listed in installation guide (or newer).
Loading lpfc or lpfcdfc driver on SLES 10 reports "unsupported module, tainting kernel" in system log.	This message is logged by the kernel whenever a module which is not shipped with the kernel is loaded. This message can be ignored.
rmmod of lpfc driver hangs and module reference count is 0.	Due to a small race condition in the kernel it is possible for an rmmod command to hang. Issue the `rmmod -w` command. If this does not help, reboot the computer.
System panics when booted with a failed HBA installed.	Remove the failed HBA and reboot.
lpfc driver unload on SLES 10 causes messages like the following to be logged in the system log: "umount: /dev/disk/bypath/pci-0000:02:04.0-scsi-0:0:1:0: not mounted"	These messages are normal output from the SLES 10 hotplug scripts and can be safely ignored.

Table 5: General Driver and HBAnyware Situations (Continued)

Situation	Resolution
rmmod fails to unload driver due to Device or resource busy. This message occurs when you attempt to remove the driver without first stopping the HBAnyware utility, when the HBAnyware utility is installed and running or when FC disks connected to a LightPulse HBA are mounted.	Stop the HBAnyware utility before attempting to unload the driver. The script is located in the /usr/sbin/hbanyware directory. Type: ./stop_hbanyware Unmount any disks connected to the HBA. Unload the driver. Type: rmmod lpfcdfc Type: rmmod lpfc
Driver Install Fails. The lpfc-install script fails to install the driver.	The install script may fail for the following reasons: • A previous version of the driver is installed. Run the lpfc-install --uninstall script and then try to install the driver. • The current driver is already installed. • The kernel source does not match the standard kernel name or you are running a custom kernel.
"No module lpfc found for kernel" error message. When upgrading the kernel, rpm generates the following error: "No module lpfc found for kernel KERNELVERSION". **A recently upgraded kernel cannot find the ramdisk.** After upgrading the kernel, the kernel cannot find the ramdisk which halts or panics the system. **The driver is not loaded after a system reboot after upgrading the kernel.**	These three situations may be resolved by upgrading the kernel. There are two ways to install the driver into an upgraded kernel. The method you use depends on whether or not you are upgrading the driver. • Upgrade the kernel using the same version of the driver. • Upgrade the kernel using a new version of the driver. See the Installation section for these procedures.
Driver uninstall fails. The lpfc-install --uninstall script fails with an error.	Try the following solutions: • Uninstall the HBAnyware and SSC software packages. These can be removed by running the ./uninstall script from the HBAnyware installation directory. • Unmount all FC disk drives. • Unload the lpfcdfc and lpfc driver.
lpfc-install script exit code.	The lpfc-install script contains exit codes that can be useful in diagnosing installation problems. See the lpfc-install script for a complete listing of codes and definitions.
The HBAnyware software package will not install. An error message states that: "inserv Service Elxlpfc has to be enabled for service ElxDiscSrvinserv: exiting now/sbin/ inserv failed exit code 1."	Reinstall the driver with the lpfc-install script.

Table 5: General Driver and HBAnyware Situations (Continued)

Situation	Resolution
The Emulex driver for Linux does not load in ramdisk for a custom built kernel.	Custom built kernels are not supported by Emulex. However, the Emulex install script will attempt to install the driver into a ramdisk that follows the naming scheme used by Red Hat or SLES kernels. • The SLES naming scheme for IA64 ramdisk images is: /boot/efi/efi/suse/initrd. • The SLES naming scheme for ramdisk images on all other architectures is: /boot/initrd. If a custom built kernel has a ramdisk image that does not follow the appropriate naming scheme, the name of the image can be changed using the following procedure: 1. Change the name of the ramdisk image to match the SLES naming scheme. 2. Update any file links to the ramdisk image. 3. Edit the boot loader configuration file: (i.e., /etc/lilo.conf, /etc/yaboot.conf, /boot/grub/grub.conf, /boot/grub/menu.lst), find any references to the old ramdisk image name, and replace them with the new name. 4. Reboot the system to verify the changes. 5. Install the Emulex lpfc Linux driver kit.
The Linux SCSI subsystem only sees 8 LUNs when more are present.	Some SCSI drivers will not scan past 8 LUNs when the target reports as a SCSI-2 device. Force SCSI bus scan with /usr/sbin/ lpfc/lun_scan. SuSE supplies /bin/rescan-scsi-bus.sh which can be changed to scan everything.
Cannot See Any HBAs. You launch the HBAnyware utility and no HBAs are visible.	Try the following solutions: • Perform an 'lsmod' to see if the Emulex drivers (lpfc and lpfcdfc) are loaded. Look for an error message on the command line stating the lpfcdfc driver is not loaded. If this is the case, do a modprobe of the lpfc and lpfcdfc drivers and relaunch the HBAnyware utility. • Exit the HBAnyware utility and run ../stop_hbanyware. Then run ./ start_elxhbamgr and ./start_elxdiscovery, and re-launch the HBAnyware utility. The HBAs should be visible. If they are not visible reboot your system.
Cannot See Other HBAs or Hosts. Although the HBAnyware utility is installed, only local host bus adapters (HBAs) are visible. The other HBAs and hosts in the SAN cannot be seen.	All the HBAs in the SAN will be visible if: • The other servers have a connection to your zone of the SAN. Check fabric zoning. • The elxhbamgr processes are running on remote hosts (enter ps -ef | grep elxhbamgr). • All other HBAs are running the HBAnyware utility and the appropriate driver. • The other HBAs are Emulex HBAs. **Note:** The HBAnyware utility services must be running on all remote hosts that are to be discovered and managed. If the HBAnyware utility Security Configurator is running, only the master or Access group client can see the servers.

Table 5: General Driver and HBAnyware Situations (Continued)

Situation	Resolution
Cannot See Multiple Zones from the Management Server. Cannot see multiple zones on the same screen of my management server running the HBAnyware utility.	Provide a physical Fibre Channel connection into each of the zones. For each zone you want to see, connect an Emulex HBAnyware utility enabled port into that zone. Use Out-of-Band discovery, Ethernet, to connect to the undiscovered server.
SAN Management Workstation Does Not Have a Fibre Channel Connection. The SAN management workstation does not have a physical Fibre Channel connection into the SAN because the other management tools are all out-of-band. Can the HBAnyware utility be run on this SAN management workstation?	The HBAnyware utility can communicate with remote HBAs using out-of-band access as long as the remote host is running HBAnyware and the remote server. To solve this problem: 1. Start the HBAnyware utility. 2. From the Main menu, select Discovery/Out-of-Band/Add Host. The Add Remote Host dialog box appears. 3. In the Add Remote Host dialog box, enter either the name or the IP-address of the host and click OK. When the selected host is discovered, that host and any HBAs running on it will be displayed in the discovery tree.
Cannot See New LUNs. Although new LUNs were created on the storage array, they do not appear in the HBAnyware utility.	Try the following: 1. Refresh the screen. 2. Exit HBAnyware and restart the HBAnyware utility. If new LUNs are visible, you are finished. If that doesn't work, try the following: 1. Exit the HBAnyware utility. 2. Navigate to /usr/sbin/hbanyware. 3. Run ./stop_hbanyware to stop both the elxhbamgr and elxdiscovery processes. 4. Run ./start_elxhbamgr and ./start_elxdiscovery to restart both processes. 5. Start the HBAnyware utility.
Unwanted Remote Servers Appear in the HBAnyware utility	To prevent unwanted servers from appearing in the HBAnyware utility, do the following: 1. Navigate to /usr/sbin/hbanyware. 2. Run ./stop_hbanyware to stop both the elxhbamgr and elxdiscovery processes. 3. Run ./start_elxhbamgr and ./start_elxdiscovery to restart both processes. Disabling this service or process prevents the local servers from being seen remotely.
The HBAnyware utility Security Configurator (Security Configurator) software package will not install. An error message states that the latest version of the HBAnyware utility must be installed first.	The system either has no HBAnyware utility software installed or has an older version of the HBAnyware utility software installed. In either case, obtain the latest version of the HBAnyware utility software and follow the installation instructions. Remember to install the HBAnyware utility software before installing the Security Configurator package.
Cannot access formerly accessible servers via the Security Configurator or the HBAnyware utility.	This is actually a symptom of two different problems. • New Keys Were Generated While Servers Were Offline • Security Removed While Servers Were Offline

Security Configurator Situations - Access Control Groups (ACGs)

Table 6: HBAnyware Security Configurator - Access Control Groups (ACG) Situations

Situation	Resolution
All servers are not displayed. When I run the Security Configurator on the Master Security Client (MSC), I do not see all of the systems in available servers or ACG Servers lists. or When I run the Security Configurator on a non-MSC, I do not see all of the systems I should see in the ACG Servers list.	Make sure all of the systems are connected to the Fibre Channel network and are online when you start the Configurator. Discovery of the systems is done only once, at startup. Unlike the HBAnyware utility, there is no Rediscover Devices button. Therefore, the Security Configurator must be restarted to rediscover new systems.
Cannot add or remove a server. The Security Configurator shows only a list of the systems in this system's ACG. I cannot add or remove systems from the ACG.	This is normal. You can modify the ACG for your system only on the MSC or on a parent client system.
HBAnyware utility shows non-ACG Servers. The HBAnyware utility shows servers that are part of the ACG and that are not part of the ACG.	The HBAnyware utility discovers unsecured servers as well as servers that are part of its ACG. The servers that you see that are not part of the ACG are unsecured. They will be discovered by any system running the HBAnyware utility on the same Fibre Channel fabric.

Security Configuration Situations - Access Sub-Groups (ASG)

Table 7: HBAnyware Security Configurator - Access Sub-Groups (ASG) Situations

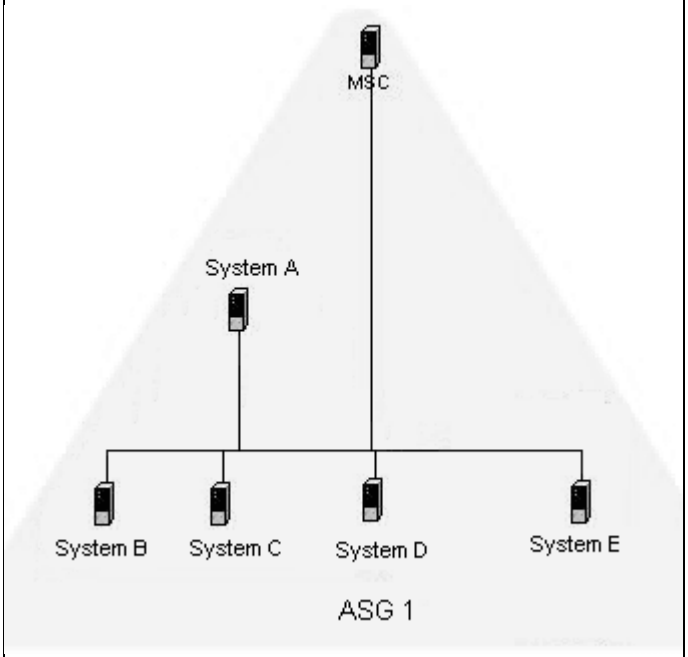
Situation	Resolution
ASG Appears to Be Non-Hierarchical. It is possible from a higher-level client (such as the MSC) to create an ASG 1 with system A as the client and systems B, C, D, and E as servers. Then create an ASG 2 with system E as the client, but with systems F and G as servers even though F and G are not part of ASG 1. This makes the topology non-hierarchical.	This scenario is shown in the following picture: System E is part of ASG 1, but has been made a client of ASG 2, and both of the servers in ASG 2 are not part of ASG 1. You could not create this ASG on system A, but you could on the MSC (or on a parent client) because it can access systems F and G. Although not shown in the picture, it is also be possible to make system A a server in ASG 2, creating a case where system A and system E are both clients and servers to/ of each other.  While the Configurator will allow you to set up ASGs this way, it is best not to create a topology like this as it can lead to confusion. The best way to set up an ASG is to set up the ASG on the MSC (or a higher-level parent) where the clients and servers do not cross over into other ASGs like in the picture. Then let the set up ASGs on clients of those ASGs in the same manner, keeping the topology hierarchical.

Table 7: HBAnyware Security Configurator - Access Sub-Groups (ASG) Situations (Continued)

Situation	Resolution
Cannot add or remove a server.	When all of the systems in an ACG are running on a single fabric, they are all available to be added to any ASG. However, if the client is connected to more than one fabric, it is possible that not all of the servers in the client's ACG are physically accessible by a chosen client for an ASG. In this case, those servers are not available to be added to that ASG. If you add a system to an ASG as a server, and then make the system a client to a child ASG, you cannot remove it from the ACG it belongs to as a server until you delete the ASG to which it is a client. Before you delete a server from an ASG, you must first remove the server from any lower level ASGs to which it belongs.
In the ASG tree of the Access Sub-Groups tab, one or more of the names of the ASGs is displayed as "- ASG (Client Offline) -".	The client system for the ASG was not discovered when the Configurator was started. This is actually a symptom of two different problems. • All Servers Are Not Displayed • New Keys Were Generated While Servers Were Offline See Table 10 on page 111 for details regarding these problems.
Not All Servers are available to an ASG. When you create a new ASG or modify an existing ASG, not all of the servers in the ACG are available to be added to the ASG.	A client system can be connected to more than one fabric. While the system the Security Configurator is running on may be able to access all of the servers in its ACG, it is not necessarily the case that the selected client for the ASG can access all of the servers. Only those that can be accessed by the selected server will be available.

HBAnyware Security Configurator Situations - Backup Masters

Table 8: HBAnyware Security Configurator - Backup Masters (BM) Situations

Situation	Resolution
Cannot create a backup master.	Select a system (or group of systems) from the MSC to be the Backup Master. The system must be either an unsecured system (which will be secured by being made a Backup Master), or a system that is not part of any ASG (client or server). These systems will mirror the MSC's security configuration. Because the Backup Master may some day take over as the MSC, the Backup Master must be able to physically access all of the systems that the MSC can access. Therefore, if the MSC is connected to multiple fabrics, the Backup Master also must be connected to those same fabrics. When you select a Backup Master, the HBAnyware Security Configurator displays a warning if it detects that the system selected to be a Backup Master is not able to physically access the same systems that the MSC can access.
Cannot modify the Security Configurator.	Select a system (or group of systems) from the MSC to be the Backup Master. The system must be either an unsecured system (which will be secured by being made a Backup Master), or a system that is not part of any ASG (client or server). These systems will mirror the MSC's security configuration. The Backup Master has client access from the HBAnyware Utility to all of the servers in the MSC's ACG. However, the Backup Master does not have client access to the MSC and it cannot modify the security configuration (create, modify or delete ASGs).
Backup Master and the MSC is no longer available. I do not have a Backup Master and the MSC system is no longer available. The servers are still secure. I installed the Security Configurator on another system, but I cannot access those servers to remove the security from them.	The servers are no longer part of a valid security configuration because there is no MSC to provide master control of the configuration. In order to reset the security on the affected servers, you will need to contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they should be seen by the Security Configurator and the HBAnyware Utility. At this point, you can set up security again through another MSC. At this time, also create a Backup Master.
The Backup Master tab is not available.	The Backup Master tab is displayed only when the Security Configurator is running on the MSC or a Backup Master. You use this tab to set up a system or systems to be backups to the MSC and to replace the MSC with a Backup Master. Each time you start the Security Configurator on the MSC and there is no Backup Master assigned, a warning message urges you to assign at least one Backup Master to prevent the loss of security information if the MSC were to become disabled.

Error Message Situations

Table 9: Error Message Situations

Situation	Resolution
The following error message is displayed when creating an ASG: “The Access Sub-Group name already exists. Please use a different name.”	You entered a duplicate ASG name in the Access Sub-Group Name field. At each level of the security topology, each ASG name must be unique. Click **OK** on the message and enter a unique ASG name.
The following error message is displayed when deleting an ASG: “The Access Sub-Group parent’s ASG is offline. You should delete the ASG when the parent ASG is available. This ASG should only be deleted if the parent ASG will not be available again. Are you sure you want to delete this ASG?”	The offline ASG entry serves as a placeholder for where the real ASG would be in the tree. You can neither modify nor delete it (although it is removed from the display if all of the child ASGs are deleted). It is possible to delete the child ASGs of the offline ASG. However, it is recommended that you delete them only if the client for the offline ASG will never be put online again. It is best to delete child ASGs when the parent ASG is online. Click **Yes** on the error message to delete the ASG or **No** to close the message without deleting.
The following error message is displayed when starting the HBAnyware Security Configurator: “This system is not allowed client access to remote servers. This program will exit.”	The system you are running the Security Configurator on is already under the security umbrella as a server to one or more clients. To make this server a client (so that it can successfully run the Security Configurator), click **OK** to close the message and exit the program, then do the following: 1. Run the Security Configurator on the MSC or on any client that has this server in its ASG. 2. Make this server a client to a group of servers.
The following error message is displayed when starting the Security Configurator: "There are no Backup Master Client Systems assigned to this security configuration. At least one should be assigned to avoid loss of the security configuration should the Master Client System become disabled."	Use the Backup Master tab to assign a Backup Master for the MSC.
The first time the Security Configurator is started in an unsecure environment, the following message is displayed: “This utility is running on an unsecure system. Continuing will allow you to set up a new security configuration making this system the Master Client System.”	Click **OK** on the message and complete the ACG setup. The system on which the Security Configurator is running will become the MSC.
When I start the Security Configurator on a Backup Master system, the following message is displayed: “Warning: This system is a backup master client system. Therefore you will only be able to view the security configuration. To make changes, you will need to run this utility on the master client system.”	Because each Backup Master system receives all the updates that the MSC makes to the security configuration, the Backup Master systems must be online when the Security Configurator is running on the MSC. Otherwise, updates to the security configuration are not reflected to the Backup Master. If the Backup Master becomes the MSC, corruption of the security configuration may occur. Click **OK** to close the message.

Master Security Client Situations

Table 10: HBAnyware Master Security Client (MSC) Situations

Situation	Resolution
The MSC is no longer bootable or able to connect to the FC network.	You must reassign a Backup Master as the new MSC from the Backup Master. **Warning:** Use this procedure **only** if the MSC cannot relinquish control to a Backup Master. For example, if the MSC is no longer bootable or able to connect to the FC network. Under any other circumstances, if the Backup Master takes over as the MSC and the MSC is still running or comes back online later, there will be two MSCs for the same security configuration. This will eventually lead to corruption of the security configuration.
New Keys Were Generated While Servers Were Offline. A "Generate New Keys" operation was performed while one or more of the servers were offline. Now those servers can no longer access the HBAnyware Security Configurator or the HBAnyware utility.	The servers are no longer part of the security configuration. In order to reset the security on the affected servers, you must contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they can be added back into the security topology by the MSC. **Note:** If the server was also a client to an ASG, then when you run the Security Configurator on the MSC or a parent client of this client, its label in the ASG tree of the Access Sub-Group tab will be "-ASG (Offline Client) -". You must delete the ASG (after deleting the child ASGs) and recreate the ASG configuration of this client and its child ASGs.
Security Removed While Servers Were Offline. Security was removed while one or more servers were offline. I can no longer access those servers from the Security Configurator or the HBAnyware utility.	The servers are no longer part of the security configuration. In order to reset the security on the affected servers, contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they should be seen by the Security Configurator or the HBAnyware utility.

lpfc Log Messages

Introducton

Log messages are organized into logical groups based on code functionality within the Fibre Channel driver. Each group consists of a block of 100 log message numbers. Most groups require a single block of 100 message numbers, however some groups (INIT, FCP) require two blocks.

The groups and the associated number ranges are defined in the Message Log table below.

Table 11: Message Log Table

LOG Message Verbose Mask Definition	From	To	Verbose Bit	Verbose Description
LOG_ELS	0100	0199	0x1	ELS events
LOG_DISCOVERY	0200	0299	0x2	Link discovery events
LOG_SLI	0300	0399	0x800	SLI events
LOG_MBOX	0300	0399	0x4	Mailbox events
LOG_INIT	0400	0499	0x8	Initialization events
Reserved	0500	0599		
LOG_IP	0600	0699	0x20	IPFC events
LOG_FCP	0700	0799	0x40	FCP traffic history
Reserved	0800	0899		
LOG_NODE	0900	0999	0x80	Node table events
LOG_CHK_COND	1000	1099	0x1000	SCSI events
Reserved	1100	1199		
LOG_MISC	1200	1299	0x400	Miscellaneous events
LOG_LINK_EVENT	1300	1399	0x10	Link events
Reserved	1400	1499		
Reserved	1500	1599		
LOG_LIBDFC	1600	1699	0x2000	IOCTL events
LOG_ALL_MSG	0100	1699	0xffff	Log all messages

Message Log Example

The following is an example of a LOG message:

```
Jul  2 04:23:34 daffy kernel: lpfc 0000:03:06.0: 0:1305 Link Down
Event x2f2 received Data: x2f2 x20 x110
```

In the above LOG message:

- lpfc 0000:03:06.0: identifies the identifies the pci location of the particular lpfc hw port.
- 0: identifies Emulex HBA0.
- 1305 identifies the LOG message number.

Note: If the word 'Data:' is present in a LOG message, any information to the right of 'Data:' is intended for Emulex technical support/engineering use only.

ELS Events (0100 - 0199)

elx_mes0100: FLOGI failure

DESCRIPTION: An ELS FLOGI command that was sent to the fabric failed.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0101: FLOGI completes successfully

DESCRIPTION: An ELS FLOGI command that was sent to the fabric succeeded.
DATA: (1) ulpWord[4] (2) e_d_tov (3) r_a_tov (4) edtovResolution
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0102: PLOGI completes to NPort <nlp_DID>

DESCRIPTION: The HBA performed a PLOGI into a remote NPort.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout (4)disc (5) num_disc_nodes
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0103: PRLI completes to NPort <nlp_DID>

DESCRIPTION: The HBA performed a PRLI into a remote NPort.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout (4) num_disc_nodes
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0104: ADISC completes to NPort <nlp_DID>

DESCRIPTION: The HBA performed a ADISC into a remote NPort.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout (4) disc (5) num_disc_nodes
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0105: LOGO completes to NPort <nlp_DID>

DESCRIPTION: The HBA performed a LOGO to a remote NPort.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout (4) num_disc_nodes
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0106: ELS cmd tag <ulpIoTag> completes

DESCRIPTION: The specific ELS command was completed by the firmware.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0107: Retry ELS command <elsCmd> to remote NPORT <did>

DESCRIPTION: The driver is retrying the specific ELS command.
DATA: (1) retry (2) delay
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0108: No retry ELS command <elsCmd> to remote NPORT <did>

DESCRIPTION: The driver decided not to retry the specific ELS command that failed.
DATA: (1) retry
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0109: ACC to LOGO completes to NPort <nlp_DID>

DESCRIPTION: The driver received a LOGO from a remote NPort and successfully issued an ACC response.
DATA: (1) nlp_flag (2) nlp_state (3) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0110: ELS response tag <ulpIoTag> completes

DESCRIPTION: The specific ELS response was completed by the firmware.
DATA: (1) ulpStatus (2) ulpWord[4] (3) nlp_DID (4) nlp_flag (5) nlp_state (6) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0111: Dropping received ELS cmd

DESCRIPTION: The driver decided to drop an ELS Response ring entry.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpTimeout
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver or firmware problem. If problems persist report these errors to Technical Support.

elx_mes0112: ELS command <elsCmd> received from NPORT <did>

DESCRIPTION: Received the specific ELS command from a remote NPort.
DATA: (1) hba_state
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0113: An FLOGI ELS command <elsCmd> was received from DID <did> in Loop Mode

DESCRIPTION: While in Loop Mode an unknown or unsupported ELS command was received.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Check device DID.

elx_mes0114: PLOGI chkparm OK

DESCRIPTION: Received a PLOGI from a remote NPORT and its Fibre Channel service parameters match this HBA. Request can be accepted.
DATA: (1) nlp_DID (2) nlp_state (3) nlp_flag (4) nlp_Rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0115: Unknown ELS command <elsCmd> received from NPORT <did>

DESCRIPTION: Received an unsupported ELS command from a remote NPORT.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Check remote NPORT for potential problem.

elx_mes0116: Xmit ELS command <elsCmd> to remote NPORT <did>

DESCRIPTION: Xmit ELS command to remote NPORT.
DATA: (1) icmd->ulpIoTag (2) hba_state
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0117: Xmit ELS response <elsCmd> to remote NPORT <did>

DESCRIPTION: Xmit ELS response to remote NPORT.
DATA: (1) icmd->ulpIoTag (2) size
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0118: Xmit ELS RPS ACC response tag <ulpIoTag>

DESCRIPTION: An RPS ACC response for the specified IO tag has been sent.
DATA:(1) ulpContext (2) nlp_DID (3) nlp_flag (4) nlp_state (5) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: None required.

elx_mes0119: Issue GEN REQ IOCB for NPORT <ulpWord[5]>

DESCRIPTION: Issue a GEN REQ IOCB for remote NPORT. These are typically used for CT request.
DATA: (1) ulpIoTag (2) hba_state
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0120: Xmit ELS RPL ACC response tag <ulpIoTag>

DESCRIPTION: An RPL ACC response for the specified IO tag has been sent.
DATA:(1) ulpContext (2) nlp_DID (3) nlp_flag (4) nlp_state (5) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: None required

elx_mes0121: PLOGI chkparm OK

DESCRIPTION: Received a PLOGI from a remote NPORT and its Fibre Channel service parameters match this HBA. Request can be accepted.
DATA: (1) nlp_DID (2) nlp_state (3) nlp_flag (4) nlp_Rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0127: ELS timeout

DESCRIPTION: An ELS IOCB command was posted to a ring and did not complete within ULP timeout seconds.
DATA: (1) elscmd (2) remote_id (3) ulpcommand (4) ulpIoTag
SEVERITY: Error
LOG: Always
ACTION: If no ELS command is going through the adapter, reboot the system; If problem persists, contact Technical Support.

elx_mes0128 - Xmit ELS ACC response tag <ulpIoTag>

DESCRIPTION: An ELS accept response for the specified IO tag has been sent.
DATA: (1) ulpContext (2) nlp_DID (3) nlp_flag (4) nlp_state (5) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0129 - Xmit ELS RJT <rejectError> response tag <ulpIoTag>

DESCRIPTION: An ELS reject response with the specified error for the specified IO tag has been sent.
DATA: (1) ulpContext (2) nlp_DID (3) nlp_flag (4) nlp_state (5) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0130 - Xmit ADISC ACC response tag <ulpIoTag>

DESCRIPTION: An ADISC ACC response for the specified IO tag has been sent.
DATA: (1) ulpContext (2) nlp_DID (3) nlp_flag (4) nlp_state (5) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0131 - Xmit PRLI ACC response tag <ulpIoTag>

DESCRIPTION: A PRLI ACC response for the specified IO tag has been sent.
DATA: (1) ulpContext (2) nlp_DID (3) nlp_flag (4) nlp_state (5) nlp_rpi
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

elx_mes0132 - Xmit RNID ACC response tag <ulpIoTag>

DESCRIPTION: A RNID ACC response for the specified IO tag has been sent.
DATA: (1) ulpContext
SEVERITY: Information
LOG: LOG_ELS verbose
ACTION: No action needed, informational.

Link Discovery Events (0200 - 0299)

elx_mes0200: CONFIG_LINK bad hba state <hba_state>

DESCRIPTION: A CONFIG_LINK mbox command completed and the driver was not in the right state.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Software driver error. If this problem persists, report these errors to Technical Support.

elx_mes0202: Start Discovery hba state <hba_state>

DESCRIPTION: Device discovery / rediscovery after FLOGI, FAN or RSCN has started.
DATA: (1) fc_flag (2) fc_plogi_cnt (3) fc_adisc_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0203: Nodev timeout on WWPN <address> NPort <nlp_DID>

DESCRIPTION: A remote NPort that was discovered by the driver disappeared for more than ELX_NODEV_TMO seconds.
DATA: (1) nlp_flag (2) nlp_state (3) nlp_rpi
SEVERITY: Error
LOG: Always
ACTION: If the device generating this message is not a target to which the HBA is connected, this error will not affect the data integrity of the I/O between the HBA and the attached storage and can be ignored.

elx_mes0204:Nodev timeout on WWPN <address> NPort <nlp_DID>

DESCRIPTION: A remote NPort that was discovered by the driver disappeared for more than ELX_NODEV_TMO seconds.
DATA: (1) nlp_flag (2) nlp_state (3) nlp_rpi
SEVERITY: Informational
LOG: LOG_DISCOVERY verbose
ACTION: If the device generating this message is not a target to which the HBA is connected, this error will not affect the data integrity of the I/O between the HBA and the attached storage and can be ignored.

elx_mes0205: Abort outstanding I/O on NPort <Fabric_DID>

DESCRIPTION: All outstanding I/Os are cleaned up on the specified remote NPort.
DATA: (1) nlp_flag (2) nlp_state (3) nlp_rpi
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0206: Device discovery completion error

DESCRIPTION: This indicates that an uncorrectable error was encountered during device (re)discovery after a link up. Fibre Channel devices will not be accessible if this message is displayed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Reboot the system. If the problem persists, report the error to Technical Support. Run with verbose mode on for more details.

elx_mes0207: Device discovery completion error

DESCRIPTION: This indicates that an uncorrectable error was encountered during device (re)discovery after a link up. Fibre Channel devices will not be accessible if this message is displayed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Reboot the system. If the problem persists, report the error to Technical Support. Run with verbose mode on for more details.

elx_mes0208: Skip <Did> NameServer Rsp

DESCRIPTION: The driver received a NameServer response.
DATA: (1) size (2) fc_flag (3) fc_rscn_id_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0209: RFT request completes ulpStatus <ulpStatus> CmdRsp <CmdRsp>

DESCRIPTION: A RFT request that was sent to the fabric completed.
DATA: None
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0210: Continue discovery with <num_disc_nodes> ADISCs to go

DESCRIPTION: A device discovery is in progress.
DATA: (1) fc_adisc_cnt (2) fc_flag (3) phba->hba_state
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0211: DSM in event <evt> on NPort <nlp_DID> in state <cur_state>

DESCRIPTION: The driver Discovery State Machine is processing an event.
DATA: (1) nlp_flag
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION:No action needed, informational.

elx_mes0212: DSM out state <rc> on NPort <nlp_DID>

DESCRIPTION: The driver Discovery State Machine completed processing an event.
DATA: (1) nlp_flag
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0214: RSCN received

DESCRIPTION: An RSCN ELS command was received from a fabric.
DATA: (1) fc_flag (2) payload_len (3) *lp (4) fc_rscn_id_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0215: RSCN processed

DESCRIPTION: An RSCN ELS command was received from a fabric and processed.
DATA: (1) fc_flag (2) cnt (3) fc_rscn_id_cnt (4) hba_state
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION:No action needed, informational.

elx_mes0217: Unknown Identifier in RSCN payload

DESCRIPTION: Typically the identifier in the RSCN payload specifies a domain, area or a specific NportID. If neither of these are specified, a warning will be recorded.
DATA: (1) un.word
SEVERITY: Error
LOG: Always
ACTION: Potential problem with Fabric. Check with Fabric vendor.

elx_mes0218: FDMI Request

DESCRIPTION: The driver is sending an FDMI request to the fabric.
DATA: (1) fc_flag (2) hba_state (3) cmdcode
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0220: FDMI rsp failed

DESCRIPTION: An error response was received to FDMI request.
DATA:(1) SWAP_DATA16(fdmi_cmd)
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: The fabric does not support FDMI, check fabric configuration.

elx_mes0221: FAN timeout

DESCRIPTION: A link up event was received without the login bit set, so the driver waits E_D_TOV for the Fabric to send a FAN. If no FAN if received, a FLOGI will be sent after the timeout.
DATA: None
SEVERITY: Warning
LOG: LOG_DISCOVERY verbose
ACTION: None required. The driver recovers from this condition by issuing a FLOGI to the fabric.

elx_mes0222: Initial FLOGI timeout

DESCRIPTION: The driver sent the initial FLOGI to fabric and never got a response back.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Check Fabric configuration. The driver recovers from this and continues with device discovery.

elx_mes0223: Timeout while waiting for NameServer login

DESCRIPTION: Our login request to the NameServer was not acknowledged within RATOV.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Check the fabric configuration. The driver recovers from this and continues with device discovery.

elx_mes0224: NameServer Query timeout

DESCRIPTION: Node authentication timeout, node Discovery timeout. A NameServer Query to the Fabric or discovery of reported remote NPorts is not acknowledged within R_A_TOV.
DATA: (1) fc_ns_retry (2) fc_max_ns_retry
SEVERITY: Error
LOG: Always
ACTION: Check Fabric configuration. The driver recovers from this and continues with device discovery.

elx_mes0225: Device Discovery completes

DESCRIPTION: This indicates successful completion of device (re)discovery after a link up.
DATA: None
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0226: Device discovery completion error

DESCRIPTION: This indicates that an uncorrectable error was encountered during device (re)discovery after a link up. Fibre Channel devices will not be accessible if this message is displayed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: Reboot the system. If the problem persists, report the error to Technical Support. Run with verbose mode on for more details.

elx_mes0227: Node Authentication timeout

DESCRIPTION: The driver has lost track of what NPORTs are being authenticated.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: None required. The driver should recover from this event.

elx_mes0228: CLEAR LA timeout

DESCRIPTION: The driver issued a CLEAR_LA that never completed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: None required. The driver should recover from this event.

elx_mes0231: RSCN timeout

DESCRIPTION: The driver has lost track of what NPORTs have RSCNs pending.
DATA: (1) fc_ns_retry (2) lpfc_max_ns_retry
SEVERITY: Error
LOG: Always
ACTION: None required. The driver should recover from this event.

elx_mes0232: Continue discovery with <num_disc_nodes> PLOGIs to go

DESCRIPTION: Device discovery is in progress.
DATA: (1) fc_plogi_cnt (2) fc_flag (3) phba->hba_state
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0234: ReDiscovery RSCN

DESCRIPTION: The number / type of RSCNs has forced the driver to go to the nameserver and re-discover all NPORTs.
DATA: (1) fc_rscn_id_cnt (2) fc_flag (3) hba_state
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0235: Deferred RSCN

DESCRIPTION: The driver has received multiple RSCNs and has deferred the processing of the most recent RSCN.
DATA: (1) fc_rscn_id_cnt (2) fc_flag (3) hba_state
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0236: NameServer req

DESCRIPTION: The driver is issuing a NameServer request to the fabric.
DATA: (1) cmdcode (2) fc_flag (3) fc_rscn_id_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0237: Pending Link Event during Discovery: State <hba_state>

DESCRIPTION: Received link event during discovery. Causes discovery restart.
DATA: None
SEVERITY: Warning
LOG: LOG_DISCOVERY verbose
ACTION: None required unless problem persists. If persistent check cabling.

elx_mes0238: Process <Did> NameServer Rsp

DESCRIPTION: The driver received a NameServer response.
DATA: (1) nlp_flag (2) fc_flag (3) fc_rscn_id_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0240: NameServer Rsp Error

DESCRIPTION: The driver received a NameServer response containing a status error.
DATA: (1) CommandResponse.bits.CmdRsp (2) ReasonCode (3) Explanation (4) fc_flag
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: Check the fabric configuration. The driver recovers from this and continues with device discovery.

elx_mes0241: NameServer rsp error

DESCRIPTION: The driver received a NameServer response containing a status error.
DATA: (1) CommandResponse.bits.CmdRsp (2) ReasonCode (3) Explanation (4) fc_flag
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: Check the fabric configuration. The driver recovers from this and continues with device discovery.

elx_mes0244: Issue FDMI request failed

DESCRIPTION: Cannot issue an FDMI request to the HBA.
DATA: (1) cmdcode
SEVERITY: Information
LOG: LOG_Discovery verbose
ACTION: No action needed, informational.

elx_mes0246: RegLogin failed

DESCRIPTION: The firmware returned a failure for the specified RegLogin.
DATA: Did, mbxStatus, hbaState
SEVERITY: Error
LOG: Always
ACTION: This message indicates that the firmware could not do RegLogin for the specified Did. There may be a limitation on how many nodes an HBA can see.

elx_mes0247: Start Discovery Timer state <hba_state>

DESCRIPTION: Start the device discovery / RSCN rescue timer.
DATA: (1) tmo (2) fc_disctmo (3) fc_plogi_cnt (4) fc_adisc_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION: No action needed, informational.

elx_mes0248: Cancel Discovery Timer state <hba_state>

DESCRIPTION: Cancel the device discovery / RSCN rescue timer.
DATA: (1) fc_flag (2) fc_plogi_cnt (3) fc_adisc_cnt
SEVERITY: Information
LOG: LOG_DISCOVERY verbose
ACTION:No action needed, informational.

elx_mes0253 - Illegal State Transition: node <nlp_DID> event <evt>, state <nlp_state>

DESCRIPTION: An unexpected response was received from the specified node.
DATA: (1) nlp_rpi (2) nlp_flag
SEVERITY: Error
LOG: Always
ACTION: Check connection to fabric and/or remove device. If problem persists, please report the issue to Technical Support.

Mailbox Events (0300 - 0399)

elx_mes0300: READ_LA: no buffers

DESCRIPTION: The driver attempted to issue a READ_LA mailbox command to the HBA, but there were no buffers available.
DATA: None
SEVERITY: Warning
LOG: LOG_MBOX verbose
ACTION: This message indicates: (1) Kernel virtual memory is depleted. Check that the system meets minimum RAM requirements for the Emulex Fibre Channel adapter. Try closing other applications to free some memory. (2) A possible driver buffer management problem. If this problem persists, report the error to Technical Support.

elx_mes0301: READ_SPARAM: no buffers

DESCRIPTION: The driver attempted to issue a READ_SPARAM mailbox command to the HBA, but there were no buffers available.
DATA: None
SEVERITY: Warning
LOG: LOG_MBOX verbose
ACTION: This message indicates: (1) Kernel virtual memory is depleted. Check that the system meets minimum RAM requirements for the Emulex Fibre Channel adapter. Try closing other applications to free some memory. (2) A possible driver buffer management problem. If the problem persists, report the error to Technical Support.

elx_mes0302: REG_LOGIN: no buffers

DESCRIPTION: The driver attempted to issue a REG_LOGIN mailbox command to the HBA, but there were no buffers available.
DATA: (1) Did (2) flag
SEVERITY: Warning
LOG: LOG_MBOX verbose
ACTION: This message indicates: (1) Kernel virtual memory is depleted. Check that the system meets minimum RAM requirements for the Emulex Fibre Channel adapter. Try closing other applications to free some memory. (2) A possible driver buffer management problem. If the problem persists, report the error to Technical Support.

elx_mes0303: Ring <ringno> handler: portRspPut <portRspPut> is bigger then rsp ring <portRspMax>

DESCRIPTION: The port rsp ring put index is larger than the size of the rsp ring.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

elx_mes0304: Stray mailbox interrupt, mbxCommand <mbxcommand> mbxStatus <mbxstatus>

DESCRIPTION: Received a mailbox completion interrupt and there are no outstanding mailbox commands.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0305: Mbox cmd cmpl error - RETRYing

DESCRIPTION: A mailbox command completed with an error status that causes the driver to reissue the mailbox command.
DATA: (1) mbxCommand (2) mbxStatus (3) un.varWords[0] (4) hba_state
SEVERITY: Information
LOG: LOG_MBOX verbose, LOG_SLI verbose
ACTION: No action needed, informational.

elx_mes0306: CONFIG_LINK mbxStatus error <mbxStatus> HBA state <hba_state>

DESCRIPTION: The driver issued a CONFIG_LINK mbox command to the HBA that failed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a firmware or hardware problem. Report these errors to Technical Support.

elx_mes0307: Mailbox cmd <mbxCommand> Cmpl <mbox_cmpl>

DESCRIPTION: A mailbox command completed.
DATA: (1) pmbox (2) varWords[0], (3) varWords[1], (4) varWords[2], (5) varWords[3], (6) varWords[4], (7) varWords[5], (8) varWords[6], (9) varWords[7]
SEVERITY: Information
LOG: LOG_MBOX verbose, LOG_SLI verbose
ACTION: No action needed, informational.

elx_mes0308: Mbox cmd issue - BUSY

DESCRIPTION: The driver attempted to issue a mailbox command while the mailbox was busy processing the previous command. The processing of the new command will be deferred until the mailbox becomes available.
DATA: (1) mbxCommand (2) hba_state (3) sli_flag (4) flag
SEVERITY: Information
LOG: LOG_MBOX verbose, LOG_SLI verbose
ACTION: No action needed, informational.

elx_mes0309: Mailbox cmd <mbxcommand> issue

DESCRIPTION: The driver is in the process of issuing a mailbox command.
DATA: (1) hba_state (2) sli_flag (3) flag
SEVERITY: Information
LOG: LOG_MBOX verbose, LOG_SLI verbose
ACTION: No action needed, informational.

elx_mes0310: Mailbox command <mbxcommand> timeout

DESCRIPTION: A mailbox command was posted to the adapter and did not complete within 30 seconds.
DATA: (1) hba_state (2) sli_flag (3) mbox_active
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver or firmware problem. If no I/O is going through the adapter, reboot the system. If the problem persists, report the error to Technical Support.

elx_mes0311: Mailbox command <mbxcommand> cannot issue

DESCRIPTION: The driver is in the wrong state to issue the specified command.
DATA: (1) hba_state (2) sli_flag (3) flag
SEVERITY: Information
LOG: LOG_MBOX verbose, LOG_SLI verbose
ACTION: No action needed, informational.

elx_mes0313: Ring <ringno> handler: unexpected Rctl <Rctl> Type <Type> received

DESCRIPTION:The Rctl/Type of a received frame did not match any for the configured masks for the specified ring.
DATA: None
SEVERITY: Warning
LOG: LOG_SLI verbose
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

elx_mes0315: Ring <ringno> issue: portCmdGet <local_getidx> is bigger then cmd ring <max_cmd_idx>

DESCRIPTION: The port cmd ring get index is greater than the size of cmd ring.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

elx_mes0317: iotag <ulp_IoTag> is out of range: max iotag <max_iotag> wd0 <wd0>

DESCRIPTION: The IoTag in the completed IOCB is out of range.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

elx_mes0318: Failed to allocate IOTAG. last IOTAG is <last_allocated_iotag>

DESCRIPTION: The driver cannot allocate an IoTag. Display the last value used.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This message indicates the adapter HBA I/O queue is full. Typically this happens when heavy I/O is running on a low-end (3 digit) adapter. We suggest you upgrade to a higher-end adapter.

elx_mes0319: READ_SPARAM mbxStatus error <mbxStatus> hba state <hba_state>

DESCRIPTION: The driver issued a READ_SPARAM mbox command to the HBA that failed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a firmware or hardware problem. Report these errors to Technical Support.

elx_mes0320: CLEAR_LA mbxStatus error <mbxStatus> hba state <hba_state>

DESCRIPTION: The driver issued a CLEAR_LA mbox command to the HBA that failed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a firmware or hardware problem. Report these errors to Technical Support.

elx_mes0321: Unknown IOCB command

DESCRIPTION: Received an unknown IOCB command completion.
DATA: (1) type (2) ulpCommand (3) ulpStatus (4) ulpIoTag (5) ulpContext)
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver or firmware problem. If these problems persist, report these errors to Technical Support

elx_mes0322: Ring <ringno> handler: unexpected completion IoTag <IoTag>

DESCRIPTION:The driver could not find a matching command for the completion received on the specified ring.
DATA: (1) ulpStatus (2) ulpWord[4] (3) ulpCommand (4) ulpContext
SEVERITY: Warning
LOG: LOG_SLI verbose
ACTION:This error could indicate a software driver or firmware problem. If problems persist report these errors to Technical Support.

elx_mes0323: Unknown Mailbox command <mbxCommand> Cmpl

DESCRIPTION: A unknown mailbox command completed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

elx_mes0324: Config port initialization error, mbxCmd <mbxCommand> READ_NVPARM, mbxStatus <mbxStatus>

DESCRIPTION: A read nvparams mailbox command failed during port configuration.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

elx_mes0325 - Reset HBA

DESCRIPTION: An HBA has been reset.
DATA: (1) hba_state (2) sli_flag
SEVERITY: Information
LOG: LOG_SLI verbose
ACTION: No action needed, informational.

elx_mes0330: IOCB wake NOT set

DESCRIPTION: The completion handler associated with the IOCB was never called.
DATA:(1) timeout (2) timeleft/jiffies
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. If the problem persists, report the error to Technical Support.

elx_mes0331: IOCB wake signaled

DESCRIPTION: The IOCB completed successfully.
DATA: None
SEVERITY: Information
LOG: LOG_SLI verbose
ACTION: None required.

elx_mes0332: IOCB wait issue failed

DESCRIPTION: The lpfc driver failed to issue an IOCB.
DATA:(1) retval
SEVERITY: Information
LOG: LOG_SLI verbose
ACTION: None required.

elx_mes0334: Unknown IOCB command

DESCRIPTION: Received an unknown IOCB command completion.
DATA: (1) type (2) ulpCommand (3) ulpStatus (4) ulpIoTag (5) ulpContext)
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver or firmware problem. If these problems persist, report these errors to Technical Support.

elx_mes0335: Unknown IOCB command

DESCRIPTION: Received an unknown IOCB command completion.
DATA: (1) ulpCommand (2) ulpStatus (3) ulpIoTag (4) ulpContext)
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver or firmware problem. If these problems persist, report these errors to Technical Support

elx_mes0336 - Rsp Ring <ringno> error: IOCB

DESCRIPTION: An IOCB error has occurred on the specified ring.
DATA: (1) ulpWord[0] (2) ulpWord[1] (3) ulpWord[2] (4) ulpWord[3] (5) ulpWord[4] (6) ulpWord[5] (7) irsp+6 (8) irsp+7
SEVERITY: Warning
LOG: LOG_SLI verbose
ACTION: If the problem persists, check the targets. If the targets are okay, report the error to Technical Support.

elx_mes0337 - Rsp Ring <ringno> error: IOCB

DESCRIPTION: An IOCB error has occurred on the specified ring.
DATA: (1) ulpWord[0] (2) ulpWord[1] (3) ulpWord[2] (4) ulpWord[3] (5) ulpWord[4] (6) ulpWord[5] (7) irsp+6 (8) irsp+7
SEVERITY: Warning
LOG: LOG_SLI verbose
ACTION: If the problem persists, check the targets. If the targets are functioning properly, report the error to Technical Support.

elx_mes0338: Kill HBA

DESCRIPTION: The driver is sending a Kill Board mailbox command to the FW..
DATA:(1) hba_state (2) sli_flag
SEVERITY: Informational
LOG: LOG_SLI verbose
ACTION: No action needed. Informational.

Initialization Events (0400 - 0499)

elx_mes0405: Service Level Interface (SLI) 2 selected

DESCRIPTION: A CONFIG_PORT (SLI2) mailbox command was issued.
DATA: None
SEVERITY: Information
LOG: LOG_INIT verbose
ACTION: No action needed, informational.

elx_mes0410: Cannot find virtual addr for mapped buf on ring <ringno>

DESCRIPTION: The driver cannot find the specified buffer in its mapping table. Thus it cannot find the virtual address needed to access the data.
DATA: (1) phys (2) next (3) prev (4) postbufq_cnt
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver or firmware problem. If problems persist report these errors to Technical Support.

elx_mes0436: Adapter failed to init, timeout, status reg <status>

DESCRIPTION: The adapter failed during powerup diagnostics after it was reset.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0437: Adapter failed to init, chipset, status reg <status>

DESCRIPTION: The adapter failed during powerup diagnostics after it was reset.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0438: Adapter failed to init, chipset, status reg <status>

DESCRIPTION: The adapter failed during powerup diagnostics after it was reset.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0439: Adapter failed to init, mbxCmd <mbxCommand> READ_REV, mbxStatus <mbxStatus>

DESCRIPTION: Adapter initialization failed when issuing a READ_REV mailbox command.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0440: elx_mes0440: Adapter failed to init, READ_REV has missing revision information

DESCRIPTION: A firwmare revision intialization error was detected.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. Update the firmware. If the problem persists, report the error to Technical Support.

elx_mes0441: VPD not present on adapter, mbxCmd <mbxCommand> DUMP VPD, mbxStatus <mbxStatus>

DESCRIPTION: The DUMP_VPD mailbox command failed.
DATA: None
SEVERITY: Information
LOG: LOG_INIT verbose
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0442: Adapter failed to init, mbxCmd <mbxCommand> CONFIG_PORT, mbxStatus <mbxStatus>

DESCRIPTION: Adapter initialization failed when issuing a CONFIG_PORT mailbox command.
DATA: (1) hbainit
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0446: Adapter failed to init, mbxCmd <mbxCommand> CFG_RING, mbxStatus <mbxStatus>, ring <num>

DESCRIPTION: Adapter initialization failed when issuing a CFG_RING mailbox command.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0447: Adapter failed init, mbxCmd <mbxCommand> CONFIG_LINK mbxStatus <mbxStatus>

DESCRIPTION: Adapter initialization failed when issuing a CONFIG_LINK mailbox command.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0448: Adapter failed to init, mbxCmd <mbxCommand> READ_SPARM, mbxStatus <mbxStatus>

DESCRIPTION: Adapter initialization failed when issuing a READ_SPARM mailbox command.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0449: lpfc_%attr attribute cannot be initialized to %d, allowed range is [%min, %max]

DESCRIPTION: Sysfs attribute value written exceeds attribute range
DATA: (1) attribute name (2) value written (3) minimum value (3) maximum value
SEVERITY: Error
LOG: Always
ACTION: Write a value within the supported range.

elx_mes0450: lpfc_%attr attribute cannot be set to %d, allowed range is [%min, %max]
DESCRIPTION: Sysfs attribute value written exceeds attribute range
DATA: (1) attribute name (2) value written (3) minimum value (3) maximum value
SEVERITY: Error
LOG: Always
ACTION: Write a value within the supported range.

elx_mes0451: Enable interrupt handler failed

DESCRIPTION: The driver attempted to register the HBA interrupt service routine with the host operating system, but failed.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or driver problem. If the problem persists, report the error to Technical Support.

elx_mes0453: Adapter failed to init, mbxCmd <mbxCommand> READ_CONFIG, mbxStatus <mbxStatus>

DESCRIPTION: Adapter initialization failed when issuing a READ_CONFIG mailbox command.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0454: Adapter failed to init, mbxCmd <mbxCommand> INIT_LINK, mbxStatus <mbxStatus>

DESCRIPTION: Adapter initialization failed when issuing an INIT_LINK mailbox command.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0455: Vital Product

DESCRIPTION: Vital product data (VPD) contained in the HBA flash.
DATA: (1) vpd[0] (2) vpd[1] (3) vpd[2] (4) vpd[3]
SEVERITY: Information
LOG: LOG_INIT verbose
ACTION: No action needed, informational.

elx_mes0457: Adapter Hardware Error

DESCRIPTION: The driver received an interrupt indicting a possible hardware problem.
Data: (1) status (2) status1 (3) status2
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a hardware or firmware problem. If the problem persists, report the error to Technical Support.

elx_mes0458: Bring adapter online

DESCRIPTION: The FC driver has received a request to bring the adapter online. This may occur when running lputil.
DATA: None
SEVERITY: Warning
LOG: LOG_INIT verbose
ACTION: None required.

elx_mes0460: Bring adapter offline

DESCRIPTION: The FC driver has received a request to bring the adapter offline. This may occur when running lputil.
DATA: None
SEVERITY: Warning
LOG: LOG_INIT verbose
ACTION: None required.

elx_mes0462: Too many cmd / rsp ring entries in SLI2 SLIM

DESCRIPTION: The configuration parameter for Scan-down is out of range.
DATA: (1) totiocb (2) MAX_SLI2_IOCB
SEVERITY: Error
LOG: Always
ACTION: This is a software driver error. If this problem persists, report these errors to Technical Support.

elx_mes0466: Too many cmd / rsp entries in SLI2 SLIM

DESCRIPTION: The driver has configured too many command and response IOCBs in all rings.
DATA: (1) total configured IOCBs (2) maximum number allowed.
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a software driver, firmware or hardware problem. Report these errors to Technical Support.

FARP Events (0600 - 0699)

elx_mes0600: FARP-RSP received from DID <did>

DESCRIPTION: A FARP response was received.
DATA: None
SEVERITY: Information
LOG: LOG_IP verbose
ACTION: None required.

elx_mes0601: FARP-REQ received from DID <did>

DESCRIPTION: An unsolicited FARP request was received.
DATA: None
SEVERITY: Information
LOG: LOG_IP verbose
ACTION: None required.

FCP Traffic History (0700 - 0799)

elx_mes0700: SCSI layer issued LUN reset (<target>,<LUN>)

DESCRIPTION: The SCSI layer is requesting the driver to abort I/O to a specific LUN.
DATA: (1) ret (2) status (3) result
SEVERITY: Error
LOG: Always
ACTION: Check the state of the target in question.

elx_mes0702: Issue Target Reset to TGT <num>

DESCRIPTION: The SCSI layer detected that it needs to abort all I/O to a specific target. This results in an FCP Task Management command to abort the I/O in progress.
DATA: (1) rpi (2) flags
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.

elx_mes0703: Issue LUN Reset to TGT <num> LUN <num>

DESCRIPTION: The SCSI layer detected that it must abort all I/O to a specific device. This results in an FCP Task Management command to abort the I/O in progress.
DATA: (1) rpi (2) flags
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: Check the state of the device in question.

elx_mes0704: At limitation of <total> preallocated command buffers.

DESCRIPTION: The maximum number of command buffers have already been allocated.
DATA: None
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: None required.

elx_mes0705: Allocation request of <num> command buffers will exceed max of <hba_queue_depth>. Reducing allocation request to <size>

DESCRIPTION: The number of command buffers requested will exceed the maximum so a smaller quantity will be allocated.
DATA: None
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: None required.

elx_mes0706: Failed to allocate command buffer.

DESCRIPTION: There was not enough memory on the system to allocate a command buffer.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: This error could indicate a heavily loaded system or a memory leak. If the problem persists, report the error to Technical Support.

elx_mes0707: driver's buffer pool is empty, IO busied.

DESCRIPTION: Resources were not available to process an IO request. A busy status will be returned.
DATA: None
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: None required.

elx_mes0710: Iodone <target>/<lun>cmd <cmd> error <result> SNS <lp> <lp3>

DESCRIPTION: This error indicates that the Fibre Channel driver is returning a SCSI command to the SCSI layer in error or with sense data.
DATA: (1) retry (2) resid
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: None required.

elx_mes0711: detected queue full - lun queue depth adjusted to %d

DESCRIPTION: The driver detected a queue full status on a scsi command response. New lun queue depth is reported
DATA: (1) New lun queue depth
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: This may indicate an oversubscribed target array. Check your SAN configuration and IO workload.

elx_mes0714: SCSI layer issued bus reset

DESCRIPTION: The SCSI layer is requesting the driver to abort all I/Os to all targets on this HBA.
DATA: (1) ret
SEVERITY: Error
LOG: Always
ACTION: Check the state of the targets in question.

elx_mes0715 - Bus Reset I/O flush failure: cnt <cnt> left <index>

DESCRIPTION: Timed out while waiting during a bus reset.
DATA: none
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: If other errors are also occurring, please report this message to Technical Support.

elx_mes0716: FCP read underrun, expected <len>, residual <resid>

DESCRIPTION: An FCP device provided less data than was requested.
DATA: (1) fcpi_parm (2) cmnd[0] (3) underflow
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: None required.

elx_mes0717: FCP command <cmd> residual underrun converted to error

DESCRIPTION: The driver converted this underrun condition to an error based on the underflow field in the SCSI command.
DATA: (1) len (2) resid (3) underflow
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: None required.

elx_mes0718 - Unable to dma_map_single request_buffer: <dma_error>

DESCRIPTION: An error occurred while sending a command, and the command will be retried.
DATA: none
SEVERITY: Error
LOG: Always
ACTION: If the problem persists, please report the error to Technical Support.

elx_mes0719 - LUN Reset I/O flush failure: cnt <cnt>

DESCRIPTION: Timed out while waiting during a LUN reset.
DATA: none
SEVERITY: Information
LOG: LOG_FCP verbose
ACTION: If other errors are also occurring, please report this message to Technical Support.

elx_mes0720 - FCP command <cmnd[0]> residual overrun error.

DESCRIPTION: A residual overrun error has occurred while processing the specified FCP command.
DATA: (1) request_bufflen (2) resid
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: If the problem persists, please check the targets for errors.

elx_mes0729: FCP cmd <cmnd> failed <target>/<lun> status: <status> result: <result>

DESCRIPTION: The specifed device failed an FCP command.
DATA: (1) ulpContext (2) iotag
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.

elx_mes0730: FCP command failed: RSP

DESCRIPTION: The FCP command failed with a response error.
DATA: (1) resp_info (2) scsi_status (3) ResId (4) SnsLen (5) RspLen (6)rspInfo3
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.

elx_mes0734: FCP read check error

DESCRIPTION: The issued FCP command returned a read check error.
DATA: (1) fcpDl (2) rspResId (3) fcpi_parm (4) cmd[0]
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: Check the state of the target in question.

elx_mes0748: Abort handler timed out waiting for abort to complete:ret <status> D <target id> LUN <lun id>

DESCRIPTION: The abort handler timed out waiting for abort to complete.
DATA: None
SEVERITY: Error
LOG: Always
ACTION: None required.

elx_mes0749: SCSI layer issued abort device

DESCRIPTION: The SCSI layer aborted a device.
DATA: (1) ret (2) id (3) lun (4) snum
SEVERITY: Warning
LOG: LOG_FCP verbose
ACTION: None required.

Node Table Events (0900 - 0999)

elx_mes0900: Cleanup node for NPort <nlp_DID>

DESCRIPTION: The driver node table entry for a remote NPort was removed.
DATA: (1) nlp_flag (2) nlp_state (3) nlp_rpi
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0901: FIND node DID reglogin

DESCRIPTION: The driver is searching for a node table entry, on the binding list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0902: FIND node DID prli

DESCRIPTION: The driver is searching for a node table entry, on the binding list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0903: FIND node DID npr

DESCRIPTION: The driver is searching for a node table entry, on the binding list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0904: Add NPort <did> to <list> list

DESCRIPTION: The driver is putting the node table entry on the specified list.
DATA: (1) nlp_flag
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0905: FIND node DID unused

DESCRIPTION: The driver is searching for a node table entry, on the binding list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0908: FIND node DID plogi

DESCRIPTION: The driver is searching for a node table entry, on the plogi list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0929: FIND node DID unmapped

DESCRIPTION: The driver is searching for a node table entry, on the unmapped node list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0930: FIND node DID mapped

DESCRIPTION: The driver is searching for a node table entry, on the mapped node list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0931: FIND node DID adisc

DESCRIPTION: The driver is searching for a node table entry, on the binding list, based on DID.
DATA: (1) ndlp (2) nlp_DID (3) nlp_flag (4) data1
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

elx_mes0932: FIND node did <did> NOT FOUND

DESCRIPTION: The driver was searching for a node table entry based on the DID and the entry was not found.
DATA: (1) order
SEVERITY: Information
LOG: LOG_NODE verbose
ACTION: None required.

Miscellaneous Events (1200 - 1299)

elx_mes1209: C_CT request error

DESCRIPTION: The CT response returned more data than the user buffer could hold.
DATA: (1) outdmp->flag (2) 4096
SEVERITY: Information
LOG: LOG_LIBDFC verbose
ACTION: Modify the user application issuing a CT request to allow for a larger response buffer.

Link Events (1300 - 1399)

elx_mes1300: Re-establishing Link, timer expired

DESCRIPTION: The driver detected a condition where it had to re-initialize the link.
DATA: (1) fc_flag (2) hba_state
SEVERITY: Error
LOG: Always
ACTION: If numerous link events are occurring, check the physical connections to the Fibre Channel network.

elx_mes1301: Re-establishing Link

DESCRIPTION: The driver detected a condition in which it had to re-initialize the link.
DATA: (1) status (2) status1 (3) status2
SEVERITY: Information
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check the physical connections to the Fibre Channel network.

elx_mes1302: Invalid speed for this board: Reset link speed to auto: <cfg_link_speed>

DESCRIPTION: The driver is reinitializing the link speed to auto-detect.
DATA: None
SEVERITY: Warning
LOG: LOG_LINK_EVENT verbose
ACTION: None required.

elx_mes1303: Link Up Event <eventTag> received

DESCRIPTION: A link up event was received. It is also possible for multiple link events to be received together.
DATA:(1) fc_eventTag (2) granted_AL_PA (3) UlnkSpeed (4) alpa_map[0]
Detail: If link events received, log (1) last event number received, (2) ALPA granted, (3) Link speed (4) number of entries in the loop init LILP ALPA map. An ALPA map message is also recorded if LINK_EVENT verbose mode is set. Each ALPA map message contains 16 ALPAs.
SEVERITY: Error
LOG: Always
ACTION: If numerous link events are occurring, check the physical connections to the Fibre Channel network.

elx_mes1304: Link Up Event ALPA map

DESCRIPTION: A link up event was received.
DATA: (1) wd1 (2) wd2 (3) wd3 (4) wd4
SEVERITY: Warning
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check the physical connections to the Fibre Channel network.

elx_mes1305: Link Down Event <eventTag> received

DESCRIPTION: A link down event was received.
DATA: (1) fc_eventTag (2) hba_state (3) fc_flag
SEVERITY: Error
LOG: Always
ACTION: If numerous link events are occurring, check the physical connections to the Fibre Channel network.

elx_mes1307: READ_LA mbox error <mbxStatus> state <hba_state>

DESCRIPTION: The driver cannot determine what type of link event occurred.
DATA: None
SEVERITY: Information
LOG: LOG_LINK_EVENT verbose
ACTION: If numerous link events are occurring, check the physical connections to the Fibre Channel network. May indicate a possible hardware or firmware problem.

IOCTL Events (1600 - 1699)

elx_mes1601: libdfc ioctl entry

DESCRIPTION: The entry point for processing an ioctl.
DATA:(1) lpfc_cmd (2) lpfc_arg1 (3) lpfc_arg2 (4) lpfc_outsz
SEVERITY: Information
LOG: LOG_LIBDFC verbose
ACTION: None required.

elx_mes1602: libdfc ioctl exit

DESCRIPTION: The exit point for processing an ioctl.
DATA:(1) rc (2) lpfc_outsz (3) lpfc_dataout
SEVERITY: Information
LOG: LOG_LIBDFC verbose
ACTION: None required.

elx_mes1604: libdfc error

DESCRIPTION: An error occurred in the lpfcdfc ioctl module.
DATA: (1) error number index
SEVERITY: Error
LOG: Always
ACTION: Reduce the application program's SCSI send request buffer size to less then 320K bytes.